TATA STEEL LONG PRODUCTS LIMITED

(formerly known as Tata Sponge Iron Limited)

Enterprise Risk Management (ERM) Framework
Policy and Guidelines
## Revision Record Sheet

### Revision history

<table>
<thead>
<tr>
<th>Version</th>
<th>Author</th>
<th>Date</th>
<th>Revision</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### This document has been reviewed by

<table>
<thead>
<tr>
<th>Reviewer</th>
<th>Date reviewed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

### This document has been approved by

<table>
<thead>
<tr>
<th>Name</th>
<th>Signature</th>
<th>Date reviewed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Index

1  Introduction  4
2  Terms & Definitions  6
3  Purpose of manual  7
4  Enterprise Risk Management Policy  8
   4.1  Enterprise Risk Management Philosophy  8
   4.2  ERM Definition  9
   4.3  ERM Framework  9
   4.4  Objectives  9
   4.5  Scope & Applicability of ERM  10
   4.6  Key Principles of ERM Framework  10
   4.7  Components of ERM Framework  11
   4.8  Risk Management Concepts  12
5  ERM Process & Framework  14
   5.1  Establish context  14
   5.2  Risk Identification  17
   5.3  Risk Assessment and Evaluation  19
   5.4  Risk Treatment  23
   5.5  Monitor, Review and Report  26
   5.6  Managing materialised risks  28
   5.7  Relationship between Internal Audit Department and ERM Department  29
6  Risk Management Organisation structure  30
7  Reference  31
   7.1  Key Documentation/ Information relating to Risk Management process  31
   7.2  Document Management  32
8  Annexure  33
1 Introduction

Risk, as defined by ISO 31000:2009 (Risk Management - Principles and Guidelines), “is the effect of uncertainty on objectives”. Enterprise Risk Management (ERM) is an integrated approach to proactively managing risks which affect the achievement of TSIL’s (herein referred to as “TSIL” or the “Company”) vision, mission and objectives. ERM is aimed at protecting and enhancing stakeholder value by establishing a suitable balance between harnessing opportunities and containing risks.

In the current dynamically changing business environment, TSIL is exposed to a plethora of risks from strategic, regulatory, alliance, operational and financial perspectives. The Board of Directors (Board) is committed to fostering an environment within the Company that enables proactive identification, management, monitoring and reporting of various risks that the Company may need to deal with. The Company-wide ERM initiative by Board would form the basis for ongoing management of risks at TSIL.

Manage all risk:

- Manage all types of risk (business, market, operational) across the company
- Manage downside risk (threats) as well as upside risk (opportunities)

Manage risk systematically:

- Manage risks as a portfolio, not separately; optimize risk vs. return; integrate cross-department risks
- Common risk framework across departments aligned to best practices, international standards
- Accountability: every risk has an “owner”
- Standardized risk metrics and reporting
- Align risk management to corporate strategy; risks are clearly linked to affected objectives
- Manage risk at the most appropriate level through an effective risk governance structure

Through this document, the Board:

- Mandates its commitment to ERM
- Seeks to embed ERM into the Company’s culture by instilling ERM in its processes, people and technology
- Intends to align ERM fundamentals with organizational objectives
- Intends to align ERM performance indicators to organizational performance indicators

Through the establishment of an ERM framework, the Board aims to realize the following benefits:

- Enhance proactive risk management
- Facilitate risk based decision making
- Improve governance and accountability
- Enhance credibility with wide range of stakeholders (e.g. Investors, Employees, Government, Regulators, Society, etc.)
- Above all, protect and enhance stakeholder value
This document outlines the TSIL ERM policy framework. It describes the Company’s risk management processes and sets out the requirements for Management in generating risk management action. The document has two parts - a “policy” section and a “guidelines” section.

The policy sets out the rules of the Company’s risk management framework. These are the mandatory requirements established by the Board for management of risk in the Company.

The guidelines provide supporting information to assist Management in the execution of risk management processes. The corporate governance drivers behind risk management today, require new ways of reporting and monitoring the Company’s risk exposures. The guidelines have therefore been provided to assist Management in dealing with these new requirements. The guidelines are aligned to good practices recommended by the Committee of Sponsoring Organisations (COSO) for ERM and ISO 31000:2009 (Risk Management - Principles and Guidelines).
2 Terms & Definitions

Enterprise Risk Management - Enterprise Risk Management is the systematic approach to managing all risks in an organization, in order to protect and enhance value.

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

Challenges – If the event is certain to happen, or has happened the risk would by definition lead to an issue/challenge. Mostly these challenges/issues are already addressed as part of annual planning processes. A challenge is also a form of obstacle that needs to be overcome to achieve desired business outcome. These are “certain” or on-going events and hence are not to be considered or treated as risks.

Issue – An issue is ‘a present problem or concern influencing organisational objectives’. In other words, an issue is raised when something has gone or is going wrong and will affect the organization.
- an issue is a problem today
- a risk may become a problem in the future.

Risk Library – Compendium of all risk identified & detailed with only risk definition (Risk event, cause, effect) and risk scores.

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

Due Diligence of risk – Deep diving into Class A risks along with RCA & ETA.

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

Risk score – The combined product of risk likelihood & risk impact

Risk Contingency Plan – Plan B for risks in case of exigency conditions

COSO – Committee of Sponsoring Organisation

Corporate risks – Total compendium of risks at corporate level escalated from divisional/hub/business unit level

Apex Class A Risks - Top priority risks (Class A) of corporate risks

Event tree analysis (ETA) – Analysis techniques for identification of sequence of events or impacts in case of risks play out.

Root cause analysis (RCA) – Analysis techniques for identification of plausible causes that may lead to the risk event.

Early warning indicator (EWI) – Early Warning Indicators are rule based quantitative or qualitative triggers based on multiple sources of information for early identification of potentially harmful scenarios.

Risk appetite – The amount of risk the organization is willing to take in pursuit of its organizational values.
**Enterprise Risk Management Framework - Policy and Guidelines**

- **Risk dashboard** – Periodic reports or MIS for risk reporting
- **Risk workshop** – Workshops facilitate a collaborative approach to brainstorm, identify and assess top risks for the concerned unit with the inclusion of all concerned stakeholders.
- **Business drivers** – Business drivers are the factors/condition that is vital for the continued success and growth of a business
- **Blue-sky thinking** - Factors impacting business continuity, competitive advantages, regulatory environment, etc.

### 3 Purpose of manual

Standard ERM process so as to provide visibility oversight, control & discipline to drive & thereon improve the organization risk management capabilities in the changing business environment.
4 Enterprise Risk Management Policy

4.1. Enterprise Risk Management Philosophy
The Risk Management philosophy of the Company is built based on its vision and strategic goals. The Company upholds its vision:

“Tata Sponge shall endeavour to be a sustainable and learning organisation for setting a benchmark in creating value in the sponge iron business, so as to meet the aspirations of its stakeholders. It shall do so through pursuit of operational excellence and by adopting opportunities of new investments in its value chain. While doing so, Tata Sponge shall continue to remain a responsible corporate citizen.”

The Company has developed a dynamic growth strategy and is in the process of implementing robust institution building processes in pursuit of its vision and strategic goals. ERM aims at balancing the two by ensuring that key decisions with regard to strategy and institution building are commensurate with the Company’s risk appetite.

An enterprise risk management philosophy that is understood by all personnel facilitates employees’ ability to recognize and effectively manage risk. The philosophy – the entity’s beliefs about risk and how it chooses to conduct its activities and deal with risk – reflects the value the entity seeks from enterprise risk management and influences how enterprise risk management components will be applied.

Management communicates its enterprise risk management philosophy to employees through policy statements and other communications.

An Integrated Approach

TSIL has adopted an integrated approach for ERM. This approach to risk management shares a common “risk language”, shared tools and techniques and periodic assessments of the total risk profile for the entire organization. This approach is appropriate when risk factors are common across business and functional units, when units are highly interdependent, and when tools and techniques developed in one unit can be readily adapted to others.

TSIL aims to integrate risk management across the organization to support its vision and towards achieving its business objectives. This will be accomplished by:

- Embedding a common risk management framework within the organization
- Proactively identifying future uncertainties and planning for them
- Training employees to consider risks as part of their decision making process

TSIL views ERM as key enabler in achieving its objective of creating and maintaining shareholder value, for successful execution of its strategies and for considering the “risk and reward” principle in the management of all business activities.

In particular, TSIL aims to:

- develop an effective ERM framework that will provide guidance on implementing ERM processes and make it part of its day to day business
- regularly identify significant risks that adversely impact the achievement of objectives and ensure these are appropriately prioritized, reported and managed
- regularly identify potential risk of lost opportunities and minimize adverse effects
- specify roles and responsibilities within ERM framework and include them as performance parameters
Enterprise Risk Management Framework - Policy and Guidelines

• regularly communicate ERM philosophy, principles and policies and procedures at all levels of staff

4.2. Enterprise Risk management (ERM) Definition

Enterprise risk management deals with risks and opportunities affecting value creation or preservation and is defined as follows:

Enterprise Risk Management (ERM) is a process, effected by the Board of Directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect its entity’s business objectives, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of TSIL’s objectives.

4.3. Enterprise Risk Management framework

The Enterprise Risk Management framework (ERM framework) refers to a set of components that provide the foundation for designing, implementing, monitoring, reviewing and continually improving risk management throughout the Company. The ERM framework for the Company has been developed keeping in mind the needs of internal and external stakeholders. The Company’s ERM framework is based on the ‘Risk Management - Principles and Guidelines’ developed by the International Organization for Standardization (ISO 31000:2009 - Risk Management Principles and Guidelines).

In addition, several good practices recommended by the Committee of Sponsoring Organizations (COSO) for ERM have also been incorporated to further the Company’s endeavor to build world class ERM framework and processes.

4.4. Objectives

TSIL Enterprise Risk Management (“ERM”) Framework provides guidance to implement a consistent, efficient, and economical approach to identify, evaluate and respond to key risks that may impact business objectives.

TSIL’s enterprise risk management framework is directed to enable management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value. Broadly, it encompasses:

• Promoting risk awareness throughout the company
• Defining risk appetite
• Identifying and managing multiple and cross-enterprise risks
• Identifying risk management team with clearly defined roles and responsibilities
• Formalizing risk response decisions
• Reducing operational surprises and losses
• Formalizing a process for identifying opportunities arising out of risk situations
• Improving deployment or more efficient use of capital and resources

ERM will help TSIL in managing risks in a proactive manner towards achieving its business objectives, performance & profitability targets and prevent loss of resources. TSIL’s ERM is directed to help ensure effective reporting and compliance with laws and regulations, avoid damage to the entity’s reputation and its consequences.
In summary, ERM is aimed to act as a process that would help TSIL to manage its risks in a structured manner with an objective to get to where it wants to go and avoid pitfalls and surprises along the way.

4.5. Scope & Applicability of ERM

The ERM framework is applicable to all aspects of TSIL’s business. This framework needs to be followed at all its Departments/locations.

4.6. Key principles of ERM Framework

The guiding principles of TSIL’s Risk Management Framework are as follows:

- Risk Management should be a continuous process.
- Risk Management principles should be kept in mind during the strategy and objective setting processes as well as the day-to-day activities and decision-making
- Risks should be understood and prioritized based on the event frequency and impact to one or more objectives
- The same metrics used to measure objectives e.g., revenue, customer satisfaction metrics, are to be preferably leveraged during risk management activities
- Risk response strategies are to be evaluated for those risks deemed to be high or medium priority
- Key risk management information (e.g., key events, results of risk assessments, risk responses) is to be documented in a timely and structured manner
- Policies, procedures and practices should be in synchronization with risks
- A portfolio view of risks is to be reviewed by the Board, Audit Committee, Management Team and Chief Risk Officer on a regular basis

4.7. Components of ERM Framework

TSIL’s Risk Management Framework comprises of:
Strategy: Strategy is critical to the framework and results in:
- Clearly defined business objectives
- Well defined risk appetite (how much risk should be taken to achieve business objectives)
- A risk profile aligned with the business strategy

Policy: It defines the guidance and standards to support strategy, consistent with the risk appetite and encompasses the following:
- Well defined roles and accountabilities for management
- Properly documented policies and procedures in line with the business needs and strategy

Infrastructure: Risk infrastructure is a set of tools to facilitate the execution of risk management objectives and comprises of:
- Enablers like technology and systems
- A robust information system that helps management in tracking risks
- Appropriate and relevant guidance that helps management to rate risks and prioritize the treatment of risks

Processes: Processes are developed to support the risk strategy and infrastructure. Processes are intended to work within the organizational context. Development and implementation of risk processes encompasses the following:
- Procedures that ensure that all risks are considered in a timely manner
- Processes to ensure that all risks are captured, assessed and responded to in a timely manner

Organization: Organizational structure is aimed at efficiently executing the strategy by means of leveraging the infrastructure and processes. Establishing an effective risk management organization should result in the following:
- Clearly defined roles and responsibilities
- Appropriate and adequate skills to manage risks
- Effective escalation of critical risk issues within the organization

Implementation of the risk management framework provides a direct link between the business strategy and risk appetite of TSIL and its systems and processes to ensure that those are designed to help TSIL meet its objectives. This framework needs to be reviewed from time to time as the business environment changes.

4.8. Risk Management Concepts

4.8.1. RISK and EVENT

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.
Event

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

4.8.2. Inherent risk vs. residual risk

Risks need to be assessed to form an appropriate response. Assessment is done first at and Inherent level (quantum of risk at this level is referred as Inherent Risk) and then at a residual level (quantum of risk at this level is referred as Residual Risk).

Inherent risk

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

Residual risk
Inherent risks may be controlled by introducing mitigating action points. 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 TSIL 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.

**4.8.3 Business Risk vs. Operational Risk**

**Business risk**

Business risk is the risk that results from your decisions about the products and services you offer. When you decide to develop and market a particular product, there's a risk that the product won't work as well as you hoped or that your marketing campaign will fail. Other business risks include changes in the cost of raw materials or shipping and managing technological developments that affect sales or manufacturing.

**Operational Risk**

Operational risks exist in the way your company tries to carry out your decisions. Operational risk rises from your company's internal decision-making and practices. Even if your business idea is sound and you have a solid customer base, an operational risk can sink your business.

**4.8.4 Risk Management as a process**

The process of Risk Management deals with how the organization

- Identifies risks that affect achievement of goals & objectives
- Measures the significance of each identified risk
- Determines the most appropriate business response to each risk
- Evaluates and reports on how well the chosen responses are being implemented

**4.8.5 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 manage risk to be within their risk appetite. Effective RM 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 and assess risks and 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 information that is reliable, timely and relevant; and
- **Satisfy legal and regulatory requirements** - Ensure compliance with legal and regulatory requirements and identify risks of non-compliance.
4.8.6. Limitations of Risk Management

Effective ERM, no matter how well designed and operated, does not guarantee achievement of all of an entity’s objectives. Achievement of objectives is affected by limitations inherent in all management processes, which include:

- **Human judgment** in decision making, which can be faulty and that breakdowns can occur because of such human failures
- Controls can be circumvented by the **collusion** of two or more individuals
- Management’s ability to **override** the risk management decisions
- Decisions on responding to risk and establishing controls depend on their related **costs and benefits**

5 ERM Process & Framework

ERM follows the 5 step process which covers process steps and components as per COSO. The structured approach is equally compatible with ISO 31000. The framework comprises of policies, processes, tools, reports and the governance structure to help the enterprise manage all the material risk and facilitate linkages between strategy risk and capital requirements.

ERM framework consists of five steps as mentioned below:

**Step 1** Establish Context
**Purpose:**
- Management sets the strategic and derived operational objectives for the organisation
- Without clear objectives there is no clear direction for Risk Management
- The risks that have to be mitigated are the risks that influence or threaten (the achievement of) the (strategic) objectives of the organisation
- Each component in the framework has to act on all objectives in order to be successful

**Process:**
Risks may arise from factors that are external to the organization. Further, in an attempt to pursue objectives, the organization might make internal changes that could result in exposure to risks. An effective ERM process takes cognizance of both external and internal context in which the Company operates. This entails understanding the external environment and internal objectives of the Company/Departments as relevant in order to ensure that risks identified are in context of the same.
**Consideration of external context**
The following are indicative factors that need to be considered/understood from an external context perspective:

- New/changes in policies or regulations that may affect the business decisions at a Sector/Company level
- Competitive landscape and position taken by competitors
- Supplier Company, partners, alliances
- Political scenario at the state and centre in India as well as the scenario in the countries where TSIL has business interests (E.g. Europe)
- Economic condition in the states/countries of operation
- Social factors that may affect the decisions pertaining to a project
- Technological changes applicable to each business

External context in which the Company operates may be determined using the following techniques:

- Porter’s five forces
- PESTLE analysis
- SWOT analysis

**Consideration of internal context**
The following need to be considered/understood from an internal context perspective:

- Strategy and objectives of the Company/Department/Corporate Services
- Inherent strengths and weaknesses/vulnerabilities of the Company/Departments.
- Organization structure and expected roles & responsibilities
- Values & beliefs
- Profile of people (qualification/experience and its relevance to their role)
- Incentive mechanisms and how it is expected to drive behaviours
- Systems and processes
- Supervision and monitoring mechanisms

**Objective Setting**
At TSIL, business/corporate objectives are set by the top management. The operating management prepares Functional/Processes level objectives that are aligned with overall corporate objectives. Every setting of objectives is an essential precondition before management can identify and assess risks with respect to them and take necessary actions to respond to those risks.

TSIL’s objectives are aligned with the entity’s risk appetite, which drives risk tolerance levels for the entity.

**Categorization of Objectives**
TSIL’s business objectives can be categorized into following:

- **Strategic** – relating to high-level goals, aligned with and supporting the entity’s vision.
- **Operations** – relating to effectiveness and efficiency of the entity’s operations, including performance and profitability goals.
- **Reporting** – relating to the effectiveness of the entity’s reporting. They include internal and external reporting and may involve financial or non-financial information.
- **Compliance** – relating to the entity’s compliance with applicable laws and regulations.
**Risk appetite**

Risk appetite defines the nature and degree of risk that an organisation will take and the risks that it will avoid in pursuit of its objectives. In other words, the Company will take risks which do not result in the breach of its appetite.

Risk appetite, established by management with oversight of the Board of Directors, is a guidepost in strategy setting. Risk appetite can be expressed as the acceptable balance of growth, risk, and return, or as risk-adjusted shareholder value-added measures. Risk appetite can be expressed in quantitative or qualitative terms.

The risk appetite statements are generally articulated under following 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

- **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
  - Reputation parameters with respect to specific stakeholders
    - Investors, analysts, lenders and rating agencies
    - Key customers
    - Key vendors/alliance partners
    - Employees
    - Media/general public

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 Company.

**Alignment of Objectives with risk appetite**

There is a relationship between an entity’s risk appetite and its strategy. ERM, applied in strategy setting, helps management select a strategy consistent with its risk appetite. If the risk associated with a strategy is inconsistent with the entity’s risk appetite, the strategy should be revised. Higher the risk appetite, more aggressive can be the strategy.

Management addresses the following questions while considering its risk appetite in setting strategies to achieve objectives:

- What risks will TSIL accept and what risks will it not accept?
- Is TSIL comfortable with the amount of risk accepted, or to be accepted, by each of its Business Functions/Processes or line of products?
- What levels of risk is TSIL prepared to accept on new initiatives in order to achieve the company-wide desired return on investment?

Refer Appendix 1 – *Risk Appetite and Risk Exposure*
5.2. Risk Identification

**Purpose:**

- Identify which events are potentially of influence on (the achievement of) the strategy and objectives.
- This step involves current as well as future events
- ERM recognizes two types of events: internal and external -
  - Internal events such as a strike, lack of quality checks or fraud control, etc.
  - External events such as an earthquake, crash of the stock market, etc.

**Process:**

Risk identification is the mechanism of identifying exposure to uncertainty across the Company. This involves assessment of the external environment within which the Company operates, as well as the internal context of the Company/Departments.

As part of risk identification, a comprehensive list of risks is generated based on events (historical and anticipated) which may prevent, degrade, accelerate or delay the achievement of business objectives. It shall also include risks associated with not identifying/evaluating opportunities pursuant to the organization’s strategic, project or business objectives, otherwise being pursued by competing organizations.

The risk causes, source, events, situations or circumstances which could have a material impact on the business objectives of the Company shall also be identified during this phase.

Risks for each Department and overall Company shall be documented in individual risk registers. The ownership of these risk registers shall lie with individual Departments; however, the ERM function shall assist in creating and updating the registers. The format for maintaining risk registers is appended in Appendix 2.

Risks once identified shall not be deleted. In case a risk becomes irrelevant, the status of the risk shall be updated to reflect the same.

Monitoring of existing risks and identification of new events on an ongoing basis is important to ensure that the inventory of events is kept current and updated. As the business environment changes over time, it is critical to have processes in place to continuously monitor and review the completeness and accuracy of the event inventory. Event identification may be carried out as and when new objectives are identified, during independent risk reviews, such as Internal Audit, Management brainstorming sessions, etc.

It shall be performed by each employee during the course of his work and particularly at the time of any significant decision, initiation of new Bid/Opportunity, during project planning and execution and periodically during the life of every operating asset. While the ERM department shall assist in risk identification, it is the responsibility of each Department to identify risks.

Risk identification involves identifying potential sources/root cause of risk events. The purpose of identifying potential root causes is to give direction to risk intervention measures. The fact that one risk might have multiple root causes also needs to be considered. As a part of the risk identification process, it is also important to understand which of the business drivers are impacted by the materialization of a risk or any of its root causes.

**Techniques of risk identification**
The following risk identification techniques can be deployed to enable focused risk identification:

- One to one interview
- Discussion with peers or internal analysis
- Questionnaires and surveys
- Workshops
- Loss event data analysis
- Monitoring external data sources
- External assistance like research groups, consultants

A combination of two or more techniques can be used for better outcome.

Risk categorization

In order to facilitate an objective assessment of identified risks, these are categorized in terms of nature of impact on the objectives. The ERM program would cover the following four main types of risks:

- Strategic risks: Risks that impact the strategic objectives of the division or Company
- Financial risks
  - Credit Risks
  - Market Risks
- Operational risks
  - Supply Chain & Operations Risks
  - IT and Security
  - HS&E
  - HRM
- Regulatory & Compliance Risks

Depending on their nature of activities, each Department in TSIL would be involved in assessing and mitigating one or more types of above risks.

There is a possibility that one element may primarily belong to one business objective and at the same time may also be mapped to an extent to another objective to some extent. This overlap depends on the facts and circumstances of each case. The process owner may decide to categorise such event to the best possible fit, which enables most effective risk management. Refer Annexure 2 for Sample Risk Categories.

5.3. Risk Assessment and Evaluation

Risk assessment

Risk assessment refers to the process followed to comprehend the nature of risk and determine the level of risk. Risk assessment is intended to provide inputs for risk evaluation.

Risk assessment provides a standard and consistent process for TSIL and its Business Units / Functions to consider the extent to which potential events might have an impact on achievement of its objectives.

It provides TSIL management with a portfolio view of risks, i.e. a “risk profile”.

During this process, events with a potential of impacting objectives are assessed and included in the overall risk profile of the respective Business Functions/Departments. Risk profiles of the various Departments are combined to form a portfolio view of risk at the Corporate level.

Risk analysis refers to the process followed to comprehend the nature of risk and determine the level of risk. Risk analysis is intended to provide inputs for risk evaluation.

Risk analysis shall be performed for each risk identified. The onus of risk analysis is with the risk identifier, who may choose to consult with the ERM department for this purpose. Based on the results of the analysis, appropriate action shall be taken (risk escalation and risk treatment).

**Techniques of risk analysis**

Risk analysis involves consideration of:

- Risk velocity – How quickly is the risk likely to manifest itself
- Likelihood of risk events – How frequently the event / risk is likely to occur
- Impact of risk – Quantum of the effect of the event / risk

**a) Risk Velocity**

No definition or reference exists on Risk velocity in ISO 31000.

- COSO Definition: Risk velocity or speed of onset refers to the time it takes for a risk event to manifest itself. "It is the time that passes between the occurrence of an event and the point at which the company first feels its effects".
- Other Definition: Velocity can be extended in other areas outside the risk assessment process. Following metrics are used to quantify the concepts
  (a) Following the risk event, time for the impact to unfold is called time to impact (TTI), or
  (b) From the known position today, time for the risk to materialise is called time to cause (TTC)
  (c) When risk event occurs and a response is initiated in order to recover from the event the time to recover from a risk event is called time to recover (TTR)

- For the purpose of ERM practice, TTI is referred to as Risk Velocity.

**Risk Velocity Score Representation, Guidelines & Tracking**

<table>
<thead>
<tr>
<th>Rating</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Very High</td>
<td>Very rapid Onset, little or no warning, instantaneous from event to impact</td>
</tr>
<tr>
<td>4</td>
<td>High</td>
<td>Onset occurs in a matter of days to a few weeks from event to impact</td>
</tr>
<tr>
<td>3</td>
<td>Medium</td>
<td>Onset occurs in a matter of a few months to a quarter from event to impact</td>
</tr>
<tr>
<td>2</td>
<td>Low</td>
<td>Onset occurs in a matter of several months to a year from event to impact</td>
</tr>
<tr>
<td>1</td>
<td>Very Low</td>
<td>Very slow onset, occurs over a year or more from event to impact</td>
</tr>
</tbody>
</table>

**b) Calculate likelihood of risk events**

The term “likelihood” is defined as a chance of something happening. This is defined, measured or determined objectively or subjectively, qualitatively or quantitatively. Likelihood may be described using general terms or even mathematically (such as a probability or a frequency over a given time period).
A realistic evaluation of risk likelihood is essential, because it guides the allocation of resources in the Company. When deciding upon a probability factor from the table (Appendix 1), the following guidelines should be considered:

- Consider how many similar incidents have occurred in the Company
- Consider, and research if necessary, how many similar incidents have occurred in the specific business segment/unit/function
- Consider the effectiveness of our existing preventative controls for the risk

c) Calculate potential impact of the identified risk scenarios

The consequences of risk are not only characterized in financial terms, the impact of the risk on various parameters detailed in the risk assessment parameters (Appendix 1) need to be calculated at this stage. Various scales of impact that are relevant according to the prevalent categories of risk such as reputation damage, personal injuries and fatalities, media coverage and operational impact must be considered during assessment of potential impact.

Assess the impact of risk across business areas

Risks do not normally exist in isolation. They usually may have a potential effect on other functions, business processes and risk categories. These cause and effect relationships must be identified and understood. This principle must become a deliberate and formal part of the risk assessment process. The results of the process must be documented. The aggregated effect of these risk Companyings and linkages should be analyzed. Many cross functional effects of risk may not be immediately apparent without deliberate and systematic analysis, so a formal approach is required.

Consolidate risks

Each Department shall arrive at a number of top risks for their respective entities. These top risks shall then be prioritized at the Department level. Similarly, top risks for all Department shall be consolidated and prioritized to arrive at a portfolio of top risks for the Company.

In order to visually depict the prioritization, a “heat map” (graphical representation of impact and likelihood) maybe used based on the risk analysis (i.e. Likelihood * Impact) wherein each risk will be plotted on the “heat map” based on its relative likelihood and impact. The placement of the risks on the “heat map” will indicate the risk zone (High/ Medium/ Low) for each of the respective risks. The heat map shall also form the basis of escalation as and when new risks are identified.

A formal risk report containing the “heat map” for the Department and the Company shall be prepared every quarter as appended in Appendix 3.

Rating Scales

A five by five matrix shall be used for measuring likelihood and impact. The risk shall be evaluated as:

Risk Measurement: Likelihood * Impact

The risk measurement scale in terms of impact and likelihood has been defined in Appendix 1 – Risk assessment parameters.

It is important to note that a single risk may impact a number of impact parameters. In such a scenario, the risk shall be evaluated for all impacts and the highest score shall be used for escalation and evaluation purposes. Once a risk has been escalated by a BU to a Segment/ Corporate, it shall be analyzed at the Segment/ Corporate level; and accordingly treated/ retained and escalated to the Company.
The risks assessed can be placed on a “heat map” which is a graphical representation of the impact and likelihood.

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Low (1)</th>
<th>Minor (2)</th>
<th>Moderate (3)</th>
<th>Major (4)</th>
<th>Critical (5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Almost certain (5)</td>
<td>Medium (5)</td>
<td>Medium (10)</td>
<td>High (15)</td>
<td>V. High (20)</td>
<td>V. High (25)</td>
</tr>
<tr>
<td>Likely (4)</td>
<td>Medium (4)</td>
<td>Medium (8)</td>
<td>Medium (12)</td>
<td>High (16)</td>
<td>V. High (20)</td>
</tr>
<tr>
<td>Possible (3)</td>
<td>Low (3)</td>
<td>Medium (6)</td>
<td>Medium (9)</td>
<td>Medium (12)</td>
<td>High (15)</td>
</tr>
<tr>
<td>Unlikely (2)</td>
<td>V. Low (2)</td>
<td>Low (4)</td>
<td>Medium (6)</td>
<td>Medium (8)</td>
<td>Medium (10)</td>
</tr>
<tr>
<td>Rare (1)</td>
<td>V. Low (1)</td>
<td>V. Low (2)</td>
<td>Low (3)</td>
<td>Medium (4)</td>
<td>Medium (5)</td>
</tr>
</tbody>
</table>

The overall risk measurement will be assessed as below:

<table>
<thead>
<tr>
<th>Likelihood*Impact (Range)</th>
<th>Risk zone</th>
<th>Risk Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Score - less than 4</td>
<td>Low</td>
<td>Class C</td>
</tr>
<tr>
<td>Score – greater than or equal to 4 but less than 12</td>
<td>Medium</td>
<td>Class B</td>
</tr>
<tr>
<td>Score – greater than or equal to 15</td>
<td>High</td>
<td>Class A</td>
</tr>
</tbody>
</table>

**Risk evaluation**

Risk evaluation is the process to determine whether the risk and/ or its magnitude is acceptable or tolerable.

The intent of risk evaluation is to:

- Enable escalation to the appropriate level of Management as per risk measurement criteria
- Prioritize for treatment implementation

Risk evaluation helps ensure appropriate resource allocation for the purpose of risk treatment and channeling of Management attention towards risks of significant concern.

Risk evaluation will involve risk prioritization for Department and the Company. Risk evaluation shall be done individually and collectively by Risk Management team / Steering Committee at various levels.

a) **Risk escalation**

A critical element of ERM is an effective system of escalation which ensures that specific issues are promptly communicated to relevant authorities. In the context of the Company, escalation may stem from one or more of the following:

- Identification of new risks at Department/ Company level
- Change in impact/ likelihood of identified risks causing a change in the risk evaluation
- Unforeseen contingencies
It is to be noted that at each level of escalation, the risk shall be reassessed so that only the key risks are filtered upwards on a timely basis.

b) Risk prioritization

The ranking of risks in terms of net potential effect provides Management with some perspective of priorities. This should assist in the allocation of capital and resources in the business. Although the scales of quantification will produce an automated ranking of risks, Management may choose to raise the rank of certain risks for other reasons. This may be justified because of non-financial influences such as media implications, social responsibilities or regulatory pressures. The ranking of risks should be shaped by strategic and business objectives. The prioritized risks must be compared with the risk appetite and all risks falling beyond the acceptable appetite must be short listed for risk treatment.

5.4. Risk Treatment

Risk treatment involves selecting one or more options for managing risks, and implementing such action plans. This phase of the ERM process is intended to:

- Understand existing controls/ mitigation mechanisms in place for managing risks
- Generate a new risk treatment plan
- Assess the effectiveness of such treatment plans

Risk mitigation relates to the policies, procedures, processes and other actionable steps implemented to address the risks associated with specified future events. Response to a risk has to be considered in light of costs to be incurred and consequent benefits (typically measured in terms of an estimate of the quantum of reduction in risk exposure).

Business risks are normal for any organization and as much as it is for TSIL. It is not the intent in all cases to minimize, avoid or eliminate all risks that are identified. However, it is the intent that all TSIL Business Units/ Functions/ Processes understand the significant events that may impact business objectives and the associated risks. This is achieved by establishing a standard and consistent process for developing an acceptable risk response.

The mitigation plan should be developed using the following steps.
The above plan would be owned by the appointed **Risk Owner**.

- Every risk should have a clearly identified owner (no gaps, no ambiguities)
- Proper risk ownership helps ensure that every identified risk is managed consistently, without duplications of effort, and in line with company objectives, improving the effectiveness and efficiency of risk management activities
- Risk owners are not necessarily the direct owners of all risk management activities in their area, but they have a control and coordination role, and are accountable for the results achieved
- Accountability for managing a risk should be assigned to the same organizational level that has the authority and responsibility to take decisions related to the corresponding objectives
- Risk owners should have sufficient “standing” in the company (department head or above)
- The decision matrix presented below supports the company in appointing the most appropriate risk owners.

Risk Mitigation Strategies can be based on the following approaches:
The choice of an appropriate treatment option must consider balancing the costs and efforts of its implementation against the benefits derived.

Steps for risk treatment:
- Evaluate the strategic mitigations in place for key risks
- Evaluate control requirements
- Verify and evaluate the controls currently in place for key risks
- Identify and evaluate the post event measures in place for risk
- Review the financial risk protection measures in place to respond to the consequences of risk events
- Take decisions on the acceptability of identified risks and controls
- Document action plans for risk mitigation
- Use the outputs of risk assessments for budgeting and capital allocation processes

Residual Risk
Residual Risk is the risk we will continue to face even if the mitigation plan works
The following are the different attributes of the residual risk:
- Impact area
- Residual Impact Score
- Residual Likelihood Score

Contingency Plan
Contingency plan is set of prioritized course of action or actions from different alternatives, which need to be implemented if an identified risk occurs.
The following are the different attributes of the contingency plan:
- Contingency plan
- Timeline
- Responsibility

For complex risks, the best response strategy requires a systematic approach to researching, evaluating, prioritizing and tracking actions:
Risk profiling

Individual risk profiles (Refer Appendix 4) shall be prepared for the prioritized risks that shall serve as a descriptive record of each key risk. Details such as risk (event, cause and impact), rationale, risk owner, treatment plans, and monitoring plans shall be maintained in the risk profile. The ERM function may assist in preparing risk profiles for each key risk. The risk profile shall be owned, regularly updated and reported to the Risk Management Committee by the risk manager/owner.

The chosen risk treatment option shall be supported by a detailed implementation plan clearly outlining:

- Activity plan clearly drafting the various steps to be performed
- Intended outcome of the activity plan
- Resource requirements to achieve successful implementation
- Accountability and responsibility for the activity plan
- Implementation time schedule
- Performance evaluation criteria to measure implementation status and the effectiveness of the treatment plan

5.5. Risk Monitor, Review and Report

Risk monitoring, review and reporting are critical components of the ERM process. The intent of monitoring and reviewing risks and their respective treatment plans is to:

- Analyze and track events, changes, trends which affect identified risks. As part of this, the impact of such events on treatment plans is also assessed
- Detecting changes and assessing the impact of changes to risk appetite, risk portfolio, risk treatment plans
- Ensure that risk treatment mechanisms are effective in design and operation
**Enterprise Risk Management Framework - Policy and Guidelines**

**Risk monitoring** shall be conducted by each Department on a **monthly basis**, for identified risks, in order to track the status of treatment plans and consequently update changes to risk profiles.

**Risk reviews** shall be conducted to enable continuity of the ERM process. Risk reviews entail the reassessment of all risks recorded in the Company, Department level risk registers along with new/emerging risks to ensure concurrence and relevance of risks and their treatment. Risk reviews will be carried out at a minimum on a **quarterly basis**.

The ERM function shall assist the monitoring and review process at the Department/Company level. The ERM function shall ensure that results of the monitoring process depicted in the form of risk reports are reported internally and externally, as appropriate.

**Early Warning Indicators (EWI)**

Early Warning Indicators are rule based quantitative or qualitative triggers based on multiple sources of information for early identification of potentially harmful scenarios.

1) **Rule based triggers**: These are triggers to flag risks early based on rules – that can be quantitative (like sharp volatility increase in energy prices) or qualitative (like change in government policies)

2) **Multiple sources of information**: The triggers could be based on internal information like supplies, labour issues, high attrition etc. or external information like raw material prices, energy markets volatility, macro-economic developments etc.

3) **Early identification**: This is the key difference between an early warning indicator vs other risk monitoring tools. These triggers raise a red-flag to warn against an impending harmful scenario early so as to enable pro-active mitigation actions.

**Designing of EWIs**

Signal strength (time between trigger and actual default) and trigger hit rate analysis is conducted to design early warning triggers.

![Diagram of Signal Strength and Trigger Hit Rate](image)

**Legend:**
- Very High Impact Triggers
- High Impact Triggers
- Medium Impact Triggers
- Low Impact Triggers
EWI monitoring depends on the kind of rules, frequency of trigger and sufficient data points for monitoring

**Kind of rules:** Low frequency rules like those based on policy changes, macro-economic factors etc. would require monitoring over a longer term as compared to rules based on shorter time-frames

**Frequency:** based on number of triggers over a given quarter/6 months/annual period, compute the hit rates and strength – if acceptable, continue using otherwise re-calibrate based on performance

**Data Points:** Would require enough data points in terms of triggers, actual events so as to analyse –
- Events that were captured by triggers – for others, develop new rules
- Trigger’ hit rates – whether triggers are actually converting to harmful events or proving to be false-alarms

5.6. **Managing materialized risks**

In the event of a particular risk materializing, it is necessary to have in place a crisis/ incident management plan for timely and effective management of such events. The incident management plan is a set of well-coordinated actions aimed at preparing and responding to unpredictable events with adverse consequences. The intention of this plan is to preserve the confidence of internal and external stakeholders in the Company’s risk readiness for potentially adverse events.

The Company recognizes the need for and shall design such a plan that will detail:
- The situations for which action plans shall be invoked
- The manner in which such plans shall be actioned
- The individuals/ departments involved in such planning and execution

5.6.1. **Loss event database**

Tracking of data pertaining to materialized risks is an essential input to the development and functioning of ERM. Such data is crucial for fine-tuning estimates of impacts of potential risks based on actual experience in the past.

The data pertaining to materialized risks shall be captured in a “Loss event database”. Typical loss events can include (but may not be restricted to):
• Environment, Health and Safety incidents
• Damage to physical assets
• Business disruption
• Fraud – internal and external
• Loss of key customers/ vendors/ alliances
• Technology/ system failures

The format for the “Loss event database” is appended in Annexure 3.

5.7. Relationship between Internal Audit department and ERM department

The Internal Audit department (IAD) plays a significant role in providing assurance on ERM activities. The operating effectiveness of risk responses shall be periodically reviewed and validated by IAD as part of the Management Assurance plans.

Outputs of risk assessments can be incorporated in developing Internal Audit plans and output of Internal Audit will be considered in developing risk treatment plans

Management of risks prioritized by Management and Audit Committee must be incorporated for review into Internal Audit plans. The risk assessment process is useful for Internal Audit staff because it provides the necessary priorities regarding risk as opposed to using standardized audit plans and programs. The audit activities will focus on adherence to controls for the key risks that have been identified. In addition, Internal Audit staff may direct Management towards the need for better controls around key risks.

In order to enable IAD to effectively leverage the ERM output and vice versa:

• ERM department shall share the list of risks identified to IAD on a need basis. IAD may use this information as an input for developing a risk based assurance plan

• IAD shall share the respective assurance reports with the ERM function on a need basis. The ERM function may use this information as an input for risk treatment plans
6. **Risk Management Organization structure**

The Company’s Enterprise Risk Management (ERM) Organization structure identifies key internal stakeholders responsible for creating, implementing and sustaining the ERM initiative in the Company. The ERM structure leverages existing organizational structure in the Company.

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

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

The Chief Risk Officer would update to the Board on a periodic basis on all key risks and work under direction of RMC (Risk Management Committee). Risk Ownerships will remain at respective Departments.

The overall structure and roles for the ERM function is summarized below
7. **Reference**

This section seeks to provide specific reference documents to the ERM practitioners, including guidelines on ERM documentation, document retention and glossary of useful terms.

### 7.1. Key Documentation

The following documents are generated during the course of the ERM exercise.

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
<th>Owner</th>
<th>Periodicity of review</th>
<th>Format reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk register</td>
<td>Record/log of information about identified risks</td>
<td>Designated Risk Owner of the Department</td>
<td>Monthly</td>
<td>Appendix 2</td>
</tr>
<tr>
<td>Risk report</td>
<td>A report/form of communication intended to inform particular stakeholders by providing information regarding the current state of key risks and its management. It is represented by a &quot;Heat Map&quot; where key risks are plotted and is supported by the detailed risk profiles</td>
<td>Risk Steering Committee</td>
<td>Quarterly</td>
<td>Appendix 4</td>
</tr>
<tr>
<td>Risk profile</td>
<td>Detailed description of a risk which is deemed priority to the Department or the Company. It shall include current risk response, and details of management action plans for further treatment including responsibilities and timelines</td>
<td>Risk owners</td>
<td>Monthly</td>
<td>Appendix 4</td>
</tr>
</tbody>
</table>
7.2. Document management

The ERM framework is owned by the Chief Risk Officer. Changes to the document need to be processed through the owner, and require the consensus of the Board for ratification.

The framework shall be reviewed annually to ensure that the intent of the same and its covenants are relevant to the Company and its entities.

The ERM department shall ensure that updates to the framework are communicated across the organization, and shall also be responsible for promoting risk awareness across the Company. The ERM function may use tools, workshops, newsletters, formal training sessions, and undertake other initiatives as deemed required for this purpose.

Record retention

For the purpose of ensuring traceability of ERM activities, documentation shall be maintained in physical or electronic form and retained as defined by the Company’s Corporate Record Retention Standards.

Records, both physical and electronic, at an Enterprise level shall be maintained by the ERM function on behalf of the Board of Directors.

However, those at the business and Sector levels shall be maintained by Department representatives designated for this purpose.
8. **Annexure**

This section collates all annexure that have been hitherto referred to in this document.

**Annexure 1: Roles and responsibilities**

**A. Board of Directors / Audit Committee**

*The Board provides oversight with regard to Risk Management and reviews the adequacy and effectiveness of business risk management as undertaken by the company*

The Board has a key role in the oversight of Risk Management. The Board should be apprised on a timely basis of the most significant risks, management’s assessment, and planned responses, if any. Importantly, the board should feel comfortable that appropriate processes are in place and that management is positioned to identify, assess, and respond to risk, and to bring relevant information to the board level.

Key roles and responsibilities are outlined below:

- Initiate and sponsor the Risk Management process and set the risk management philosophy
- Reviewing and approving risk management related policies, procedures and parameters that govern the management of the Company, Departments etc.
- Reviewing the entity’s portfolio view of risk and considering it against the entity’s risk Appetite
- Reviewing the most significant risks and appropriateness of management response
- Allocating adequate resources for treating critical risks and(or) risk events at a Company level
- Ensures the requisite systems and practices are in place to manage key risks to which the Company is exposed
- Endorsing the risk management structure and authorizing roles and responsibilities for key stakeholders
- Independent review of the ERM department and its activities pertaining to the risk management intent in form and spirit.
- Ensures that high risk areas are addressed in the internal audit plans for validation of controls
B. Managing Director

The MD leads the ERM process

The MD has ultimate ownership responsibility for ERM. The MD and Directors generally fulfil these responsibilities by setting broad-based policies reflecting the entity’s ERM philosophy and risk appetite, providing leadership, direction and guidance to Operating Management in performing ERM activities across TSIL.

Key roles and responsibilities are outlined below:

- Set business strategies in consultation with the Board
- Assist the Board / Audit Committee in meeting their responsibilities for risk management and sponsoring ERM process
- Be accountable for maintenance of an adequate ongoing risk management process
- Ensure staff at all levels are aware of the risk and control environment within each business process
- Promote risk management strategy and policy by enhancing the level of risk awareness within the Company
- Owning key risks impacting overall Company, and establishing a risk environment that is consistent with accepted practices and fulfils the expectations of the shareholders
- Reviewing the critical aspects of the Company’s overall risk profile through the periodic review of high-level reports that address material risks and strategic implications

C. Risk Management Committee

Key roles and responsibilities are outlined below:

- Recommend changes on risk appetite parameters for approval of the Board
- Ensuring risk identification and assessment for:
  - New bids and ventures (need basis)
  - Projects and operating assets (ongoing)
  - Sector/ departments/ divisions (ongoing)
- Conducting risk analysis and evaluation including:
  - Identifying root causes/ sources for individual risks
  - Assessing the impact of risks on achievement of objectives
  - Aggregating risks at a Company level
  - Comparing with risk thresholds/ appetite
- Identifying and implementing risk treatment plans and measures for residual risks
- Providing risk responses and evaluating sufficiency of existing risk treatment mechanisms
Enterprise Risk Management Framework - Policy and Guidelines

- Managing materialized risks by:
  - Initiating immediate actions for controlling the impact of the materialized risk event
  - Coordinating with corporate communications/Board for external and internal communications
- Supporting the Board/MD in Group level risk identification, assessment and treatment
- Providing necessary support to the ERM department in performing risk management activities as envisaged
- Communicating to the ERM department significant developments(changes to business and other key business decisions.
- Supporting the MD in implementing the risk mitigation strategies including:
  - Resource requirements (including contingencies)
  - Assigning ownership and responsibility for risk mitigation to various functional departments
  - Detailed activity plans, timelines and schedules
- Collaborating with Corporate Strategy and Planning department (if any), ERM and MD to ensure that the impact of risks and the treatment strategies are factored in the strategic planning process

D. ERM department – Headed by Chief Risk Officer (CRO)

The CRO works with Management Team in establishing effective ERM in their areas of responsibility.

Under the guidance of MD, the CRO co-ordinates enterprise risk management across TSIL. He acts as a facilitator by assisting Management Team in performing ERM activities, monitoring the progress and acting as a risk reporting channel.

Key roles and responsibilities are outlined below:

- Providing overall leadership to ERM process in line with directions of the Board
- Developing and assuming ownership of the risk management policy, framework and process. Implementing the ERM framework, policy and process across the Company, Departments etc.
- Establishing procedures and timelines for various risk management activities
- Provide necessary information and feedback to facilitate definition of risk thresholds at Company/Department levels.
- Liaising with Risk Management Committees at various levels for deploying the ERM process
- Facilitating risk identification, evaluation, prioritization and consolidation
- Assisting the respective Departments in the identification of risk owners for each risk
- Providing input and feedback on proposed risk treatment plans and initiatives. Also, coordinates with different functions for cross-functional mitigation measures.
Enterprise Risk Management Framework - Policy and Guidelines

- Monitoring progress of implementation of risk treatment plans and strategies
- Ensuring that risk reviews are carried out on a periodic basis in order to maintain continuity of the risk management process
- Preparing and communicating risk reports with risk mitigation measures to relevant stakeholders
- Training and collaborating with the Departments in carrying the ERM process further on a regular basis to aid management in decision making
- Promoting risk management culture through trainings, reporting and other internal communications
- Developing the analytical systems and data management capabilities to support the risk management program
- Developing an annual risk management training calendar to ensure that individuals engaged in risk management are:
  - Updated about risk management policies, processes and practices
  - Developed with appropriate risk management skills and competencies
- Reviewing significant deviations from the risk management framework or other risk management procedures and bringing it to Risk Management Committee / Board’s attention as appropriate
- Rendering support to the Risk Management Committee for effecting changes to the risk management organization and process
- Assisting with implementation of procedures for proactive review of risks for projects, transactions, new businesses, etc.
- Monitoring external trends and factors that may have significant impact on the risk profile of the Company and communicating the information to all stakeholders within the Company
- Take ownership of implementation and ongoing improvement of e-enablement initiatives for ERM function
- Developing risk management policies and proposing necessary updates

E. Risk Owners/ Mitigation Owners

- Assuming overall responsibility for managing the existing individual risk and identify new emerging risks on an ongoing basis and report to the CRO (for assessment, prioritization and response planning)
- Assuming overall responsibility for mitigating the individual risk as agreed in the risk profile
- Coordinating with the others Department and CRO in delineating an appropriate risk treatment option for the risk assigned
- Monitoring the progress of the risk treatment plans and periodically evaluating the risk against the risk threshold level
- Managing the impact of residual risks and taking appropriate measures to monitor and control the same
Enterprise Risk Management Framework - Policy and Guidelines

- Populate the Risk Register with the risk description classified under agreed risk categories along with a rating of impact and likelihood based on the rating parameters applicable
- Report on the status of risk management activities and results to Chief Risk Officer
- Report on the status of the risk and its treatment plan
- Timely escalation of challenges, concerns or unforeseen developments pertaining to the risk and/or risk mitigation measures and actions to prevent their recurrence
- Conduct periodic training programs as per guidance from Chief Risk Officer and other Departmental Heads and ensure risk awareness at all time

F. Internal Audit Department

*Internal auditors play a key role in the ongoing functioning of ERM by providing objective monitoring of its application and effectiveness.*

Internal auditors conduct examinations for the purpose of providing an objective assessment of the entire ERM process or subsets thereof. In this role, internal auditors may support management by providing assurance on:

- The design of Enterprise risk management processes and organisation structure in that respect
- Effectiveness and efficiency of risk responses and related control activities

Key roles and responsibilities are outlined below:

- Assist Senior management and Audit Committee in fulfilling responsibilities in monitoring the systems related to internal controls and risks
- Ensure Risk Management Policy has been fully complied with and implemented
- Understand the risks of the Company as identified by management and take account of such risks in audit work
- Evaluate the adequacy and effectiveness of risk responses and control activities
- Keep abreast of industry best practices and recommend such practices to the Company, where appropriate
- Communicate and share risk information gathered during the audit process with the Chief Risk Officer

Annexure 2: Sample risk categories

Risks identified and assessed can arise from multiple categories. Some sample categories are provided below:

<table>
<thead>
<tr>
<th>Risk category</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting and financial reporting</td>
<td>Potential risk arising from improper accounting or financial reporting</td>
</tr>
<tr>
<td>Credit</td>
<td>Potential risk arising from counterparty default or internal credit downgrades</td>
</tr>
<tr>
<td>Ethics/compliance</td>
<td>Potential risk arising from unethical employee actions or deviations from internal policies (e.g., Code of Conduct)</td>
</tr>
<tr>
<td>Human Resources</td>
<td>Potential risk arising from the Company’s inability to attract, retain or properly train qualified individuals</td>
</tr>
<tr>
<td>Risk category</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Information Technology</td>
<td>Potential risk arising from the failure or inadequacy of information technology</td>
</tr>
<tr>
<td>Legal</td>
<td>Potential risk arising from legal action, contractual breaches or adverse statutory modifications</td>
</tr>
<tr>
<td>Market</td>
<td>Potential risk arising from adverse market movements or liquidity constraints</td>
</tr>
<tr>
<td></td>
<td>Market risk sources:</td>
</tr>
<tr>
<td></td>
<td>• <em>Financing cost fluctuations</em> – resulting in elevated funding costs or reduced investment returns or credit rating downgrades</td>
</tr>
<tr>
<td></td>
<td>• <em>Commodity price fluctuations</em> – resulting in any given calendar year cash flow mismatch between authorized revenue requirements and cash collections</td>
</tr>
<tr>
<td></td>
<td>• <em>Foreign exchange fluctuations</em> – resulting in profit or loss on account of change in foreign exchange rates between time of incurrence of expense/ income and actual payment/ collection</td>
</tr>
<tr>
<td></td>
<td>• <em>Liquidity constraints</em> – resulting in the Company’s inability to meet short-term obligations. Liquidity constraints are generated from two primary sources: 1) an inability to sell assets (market liquidity risk) in a timely manner and 2) an inability to obtain adequate funding without incurring unacceptable losses (funding liquidity risk)</td>
</tr>
<tr>
<td>Operational</td>
<td>Potential risk arising from ineffective internal business processes and procedures, people, systems</td>
</tr>
<tr>
<td>Physical Asset</td>
<td>Unplanned and unbudgeted events impairing the Company’s physical assets and affecting the ability to generate and deliver services to its customers</td>
</tr>
<tr>
<td>Regulatory</td>
<td>Potential risk arising from industry regulatory violations or adverse regulatory amendments/ rulings/ decisions</td>
</tr>
<tr>
<td>Reputation</td>
<td>Potential reduction to equity value or market share (revenue) arising from negative publicity</td>
</tr>
<tr>
<td>Environment, Health and Safety</td>
<td>Environment: Potential risk arising from detrimental environmental (air, land, water) events (e.g., spill, emissions) related to the Company’s operations</td>
</tr>
<tr>
<td></td>
<td>Health: Potential risk arising from exposures to hazardous substance that may have damaged or will damage the health of exposed persons</td>
</tr>
<tr>
<td></td>
<td>Safety: Potential risk arising from threats or inadequate safeguards to maintain both the well-being of the Company’s human capital and the public’s safety</td>
</tr>
<tr>
<td>Strategic</td>
<td>Potential risk arising from poor business decisions, improper service or offering, inadequate physical infrastructure support or limited business analysis</td>
</tr>
<tr>
<td>Tax</td>
<td>Potential risk resulting from improper tax application, non-compliance or adverse tax rulings</td>
</tr>
<tr>
<td>Financial</td>
<td>Potential risk of cash flows generated not being adequate to meet financial obligations</td>
</tr>
<tr>
<td>Business Continuity</td>
<td>Potential risks arising from disruption to business due to natural/ man made disasters, accidents, unavailability of supporting infrastructure or people</td>
</tr>
<tr>
<td>Business Development</td>
<td>Potential risks arising from inability to identify potential opportunities, create long term partnerships with suppliers, customers or alliance partners</td>
</tr>
</tbody>
</table>