

## **RISK ASSESSMENT AND MANAGEMENT POLICY**

---

### **1. PREAMBLE**

Pursuant to Regulation 17(9) of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 (“SEBI Listing Regulations”) and Section 134(3) of the Companies Act, 2013, this Risk Assessment and Management Policy (“Policy”) establishes the philosophy of Tega Industries Limited (“Company”), towards risk identification, analysis and prioritization of risks, development of risk mitigation plans and reporting on the risk environment of the Company. This Policy is applicable to all the functions, departments and geographical locations of the Company. The purpose of this Policy is to define, design and implement a risk management framework across the Company to identify, assess, manage and monitor risks. Aligned to this purpose is to identify potential events that may affect the Company and manage the risk within the risk appetite and provide reasonable assurance regarding the achievement of the Company’s objectives. This will present a wide approach to ensure that key aspects of risk that have a wide impact are considered in its conduct of business.

**Risk:** Risk is an event which can prevent, hinder or 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.

Accordingly, the board of directors of Company (“Board”) has adopted this Policy at its meeting held on 3<sup>rd</sup> August 2021, which can be amended from time to time. The Policy has been adopted in supersession of the Enterprise Risk Management Framework adopted by the Board earlier and accordingly the Enterprise Risk Management Framework will no longer be applicable to the Company from the date of adoption of this Policy.

### **2. VISION STATEMENT**

- Tega Industries Limited recognizes that profit, stakeholder value addition etc. is the reward for taking and effectively managing risk. The Company will leverage risk management as a part of its strategic decision-making processes. Using a systematic and consistent approach, the Company will proactively identify current and emerging risks and manage those risks. The Policy will generate a detailed view of risks across Tega Industries Limited which will enable Executives to take decisions that optimally allocate resources.
- Tega Industries Limited seeks to be recognized as employing an industry-leading risk management framework.

### **3. OBJECTIVE**

The objective of this Policy is to manage the risks involved in all activities of the Company, to maximize opportunities and minimize adversity. This Policy is intended to assist in decision making processes that will minimize potential losses, improve the management of uncertainty and the approach to new opportunities, thereby helping the Company to achieve its objectives. The objectives of the Policy can be summarized as follows:

- (a) To safeguard the Company’s and its subsidiaries’/ joint ventures’ property, interests, and interest of all stakeholders;
- (b) To manage risks with an institutionalized framework and consistently achieving desired outcomes;
- (c) To protect and enhance the corporate governance;
- (d) To implement a process to identify potential / emerging risks;
- (e) To implement appropriate risk management initiatives, controls, incident monitoring, reviews and continuous

improvement initiatives;

- (f) Minimize undesirable outcomes arising out of potential risks; and
- (g) To align and integrate views of risk across the enterprise.

#### **4. COMPONENTS OF A SOUND RISK MANAGEMENT SYSTEM**

The risk management system in the Company should have the following key features:

- (a) Active board of directors, committee and senior management oversight;
- (b) Appropriate policies, procedures and limits;
- (c) Comprehensive and timely identification, measurement, mitigation, controlling, monitoring and reporting of risks;
- (d) Appropriate management information systems at the business level;
- (e) Comprehensive internal controls in accordance with current regulations; and
- (f) A risk culture and communication framework

#### **5. RISK GOVERNANCE**

An organization's ability to conduct effective risk management is dependent upon having an appropriate risk governance structure and well-defined roles and responsibilities. Risk governance signifies the way the business and affairs of an entity are directed and managed by its Board and executive management.

#### **6. RISK MANAGEMENT FRAMEWORK**

The risk management committee formed by the Board shall periodically review the risk assessment and management policy of the Company and evaluate the risk management systems so that management controls the risk through a properly defined network.

Heads of departments shall be responsible for implementation of the risk management system as may be applicable to their respective areas of functioning.

#### **7. RISK MANAGEMENT PROCESS**

Conscious that no entrepreneurial activity can be undertaken without assumption of risks and associated profit opportunities, the Company operates on a risk management process /framework aimed at minimization of identifiable risks after evaluation so as to enable management to take informed decisions.

Broad outline of the framework is as follows:

- a) Risk Identification:** Management identifies potential events that may positively or negatively affect the Company's ability to implement its strategy and achieve its objectives and performance goals. Potentially, negative events represent risks and are assigned a unique identifier. The identification process is carried out in such a way that an expansive risk identification covering operations and support functions are put together and dealt with. No one individual will possess the breadth of knowledge required to identify all the risks the company may face, the impacts they may have or the treatment strategies required to manage them. The success of this phase relies on involvement across the entire group and stakeholders. A well-structured systematic process is critical as a risk not identified at this stage may be excluded from further analysis. The aim is to develop a comprehensive list of sources of risk and events that might have an impact on company's objectives or outcomes.

Risks can be identified under the following broad categories. This is an illustrative list and not necessarily an exhaustive classification.

(i) Internal risks including:

- Strategic and Business Risk: Competition, inadequate capacity, high dependence on a single customer/vendor, project viability, process risk, technology obsolescence/ changes, development of alternative products.
- Financial Risk: Liquidity, credit, currency fluctuation.
- Operational Risk: Process bottlenecks, non-adherence to process parameters/ pre-defined rules, difficulty in meeting production targets due to improper sales planning, improper equipment planning, non-availability of raw materials/ spares on time, breakdown of machinery etc. Also, safety risks form a part of operational risks as those arise due to non-compliance to safety standards of the company which may result in loss of human life/ property.
- Reputation Risk: Brand impairment, product liabilities.
- Compliance Risk: Non-compliance to statutes, change of regulations.
- Other risks:
  - Environment Risk: Non-compliance to environmental regulations, risk of health to people at large.
  - Personnel Risk: Health & safety, high attrition rate, incompetence.

(ii) External risks including:

- Sectoral Risk: Unfavorable consumer behavior in relation to the relevant sector etc.
- Sustainability Risk: Environmental, social and governance related risks.
- Political Risk: Changes in the political environment, regulation/ deregulation due to changes in political environment.

**b) Root Cause Analysis:** Undertaken on a consultative basis, root cause analysis enables tracing the reasons / drivers for existence of a risk element and helps developing appropriate mitigation action.

**c) Risk Scoring and analysis:** Management considers qualitative and quantitative methods to evaluate the likelihood and impact of identified risk elements. Likelihood of occurrence of a risk element within a finite time is scored based on polled opinion or from analysis of event logs drawn from the past. Impact is measured based on a risk element's potential impact on cost, revenue, profit etc. should the risk element materialize. The composite score of impact and likelihood are tabulated in an orderly fashion and the table is known as a 'Risk Register'. For scale of impact and likelihood, please refer to **Annexure A**.

The resultant "action required" is derived based on the combined effect of impact & likelihood and is quantified as per the summary below.

**d) Risk Categorization:**

The identified risks are further grouped into (a) preventable; (b) strategic; and (c) external categories to homogenize risks.

(i) Preventable risks are largely internal to the Company and are operational in nature. The endeavour is to reduce /eliminate the events in this category as they are controllable. Standard operating procedures and

audit plans are relied upon to monitor and control such internal operational risks that are preventable.

- (ii) Strategy risks are voluntarily assumed risks by the senior management in order to generate superior returns / market share from its strategy. Approaches to strategy risk is 'accept'/'share', backed by a risk-management system designed to reduce the probability that the assumed risks actually materialize and to improve the Company's ability to manage or contain the risk events should they occur.
- (iii) External risks arise from events beyond organization's influence or control. They generally arise from natural and political disasters and major macroeconomic shifts. Management regularly endeavours to focus on their identification and impact mitigation through 'avoid'/'reduce' approach that includes measures like business continuity plan / disaster recovery management plan / specific loss insurance / policy advocacy etc.

**e) Risk Prioritization:**

Based on the composite scores, risks are prioritized for mitigation actions and reporting

**f) Risk Mitigation Plan:**

Management develops appropriate responsive action on review of various alternatives, costs and benefits, with a view to managing identified risks and limiting the impact to tolerance level. Risk mitigation plan drives policy development as regards risk ownership, control environment timelines, standard operating procedure, etc.

Risk mitigation plan is the core of effective risk management. The mitigation plan covers:

- (i) Required action(s);
- (ii) Required resources;
- (iii) Responsibilities;
- (iv) Timing;
- (v) Performance measures; and
- (vi) Reporting and monitoring requirements

The mitigation plan also covers (i) preventive controls - responses to stop undesirable transactions, events, errors or incidents occurring; (ii) detective controls - responses to promptly reveal undesirable transactions, events, errors or incidents so that appropriate action can be taken; (iii) corrective controls - responses to reduce the consequences or damage arising from crystallization of a significant incident.

Therefore, it is drawn with adequate precision and specificity to manage identified risks in terms of documented approach (accept, avoid, reduce, share) towards the risks with specific responsibility assigned for management of the risk events.

**g) Risk Monitoring:**

It is designed to assess on an ongoing basis, the functioning of risk management components and the quality of performance over time. Staff members are encouraged to carry out assessments throughout the year.

**h) Options for dealing with risk**

There are various options for dealing with risk.

**Tolerate** – If we cannot reduce the risk in a specific area (or if doing so is out of proportion to the risk) we can decide to tolerate the risk; i.e., do nothing further to reduce the risk. Tolerated risks are simply listed in the corporate risk register.

**Transfer** – Here risks might be transferred to other organizations, for example by use of insurance or transferring out an area of work.

**Terminate** – This applies to risks we cannot mitigate other than by not doing work in that specific area. So if a particular project is of very high risk and these risks cannot be mitigated we might decide to cancel the project.

**i) Risk Reporting:**

Periodically, key risks are reported to the Board or risk management committee with causes and mitigation actions undertaken/ proposed to be undertaken.

The internal auditor carries out reviews of the various systems of the Company using a risk based audit methodology. The internal auditor is charged with the responsibility for completing the agreed program of independent reviews of the major risk areas and is responsible to the audit committee which reviews the report of the internal auditors on a quarterly basis.

The statutory auditors carries out reviews of the Company’s internal control systems to obtain reasonable assurance to state whether an adequate internal financial controls system was maintained and whether such internal financial controls system operated effectively in the company in all material respects with respect to financial reporting.

On regular periodic basis, the Board will, on the advice of the audit committee, receive the certification provided by the CEO and the CFO, on the effectiveness, in all material respects, of the risk management and internal control system in relation to material business risks.

The Board shall 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.

**j) Risk Management Measures adopted in general by the Company:**

The Company has adopted various measures to mitigate the risk arising out of various areas described above, including but not limited to the following:

- (i) A well-defined organization structure;
- (ii) Defined flow of information to avoid any conflict or communication gap;
- (iii) Hierarchical support personnel to avoid work interruption in absence/ non-availability of functional heads;
- (iv) Discussion and implementation on financial planning with detailed business plans;
- (v) Detailed discussion and analysis of periodic budgets;
- (vi) Employees training and development programs;
- (vii) Internal control systems to detect, resolve and avoid any frauds;
- (viii) Systems for assessment of creditworthiness of existing and potential contractors/subcontractors/ dealers/vendors/ end-users;
- (ix) Redressal of grievances by negotiations, conciliation and arbitration; and
- (x) Defined recruitment policy.

**8. RESPONSIBILITY FOR RISK MANAGEMENT**

Responsibility holder	Responsibilities
Board	<p>The Company’s risk management architecture is overseen by the Board and the policies to manage risks are approved by the Board. Its role includes the following:</p> <ul style="list-style-type: none"> <li>• Ensure that the organization has proper risk management framework</li> </ul>

	<ul style="list-style-type: none"> <li>• Define the risk strategy, key areas of focus and risk appetite for the company</li> <li>• Approve various risk management policies including the code of conduct and ethics</li> <li>• Ensure that senior management takes necessary steps to identify, measure, monitor and control these risks</li> </ul>
<p style="text-align: center;">Audit Committee</p>	<p>The Audit Committee assists the Board in carrying out its oversight responsibilities relating to the Company's (a) financial reporting process and disclosure of financial information in financial statements and other reporting practices, b) internal control, and c) compliance with laws, regulations, and ethics (d) financial and risk management policies. Its role includes the following:</p> <ul style="list-style-type: none"> <li>• Setting policies on internal control based on the organisation's risk profile, its ability to manage the risks identified and the cost/ benefit of related controls;</li> <li>• Seeking regular assurance that the system of internal control is effective in managing risks in accordance with the Board's policies.</li> <li>• Ensure that senior management monitors the effectiveness of internal control system</li> <li>• Help in identifying risk, assessing the risk, policies / guidance notes to respond its risks and thereafter frame policies for control and monitoring.</li> </ul>
<p style="text-align: center;">Risk Management Committee</p>	<p>The Risk Management Committee, as constituted by the Board, is the key committee which implements and coordinates the risk function as outlined in this policy on an ongoing basis. Its role includes the following:</p> <ul style="list-style-type: none"> <li>• Ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company;</li> <li>• Monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems;</li> <li>• Periodically review the risk management policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity, and recommend for any amendment or modification thereof, as necessary;</li> <li>• Keep the Board of directors of the Company informed about the nature and content of its discussions, recommendations and actions to be taken;</li> <li>• Review the appointment, removal and terms of remuneration of the Chief Risk Officer (if any);</li> <li>• To implement and monitor policies and/or processes for ensuring cyber security; and</li> </ul> <p>any other similar or other functions as may be laid down by Board from time to time and/or as may be required under applicable law.</p>
<p style="text-align: center;">Chief Risk Officer</p>	<ul style="list-style-type: none"> <li>• Evaluating the compliance in relation to control mitigation plan and timelines and reporting to Risk Management Committee efficacy of risk management framework.</li> <li>• Initiating and coordinating activities for operationalizing the risk management framework and reporting to Risk Management Committee.</li> <li>• Periodically review the process for systematic identification and assessment of the business risks.</li> <li>• Provide inputs and recommend mitigation controls to Risk Management Committee</li> <li>• The Company Secretary of the Company will be the Chief Risk Officer of the Company.</li> </ul>

## **9. BUSINESS CONTINUITY PLAN**

The Company will formulate a Business Continuity Plan as per the requirement of the Policy and time to time will update/ revise the same as per the requirements.

## **10. COMMUNICATION AND CONSULTATION**

Appropriate communication and consultation with internal and external stakeholders should occur at each stage of the risk management process as well as on the process as a whole.

## **11. DISCLAIMER CLAUSE**

The risks outlined above are not exhaustive and are for information purposes only. Management is not an expert in assessment of risk factors, risk mitigation measures and management's perception of risks. Readers are therefore requested to exercise their own judgment in assessing various risks associated with the Company.

## **12. PERIODICAL REVIEW OF EFFECTIVENESS**

Effectiveness of risk management framework is ensured through periodical review of this Policy, provided that such review should be undertaken at least once in two years. As the risk exposure of any business may undergo change from time to time due to the changing industry dynamics, evolving complexity and continuously changing environment, the updation and review of this Policy will be done as and when required, by the risk management committee to ensure it meets the requirements of legislation and the needs of organization.

In the event of any conflict between the Companies Act, 2013 or the SEBI Listing Regulations or any other statutory enactments and the provisions of this Policy, the Regulations shall prevail over this Policy. Any subsequent amendment/modification in the SEBI Listing Regulations, in this regard shall automatically apply to this policy.

## **13. APPROVAL OF THE POLICY**

The Board will be the approving authority for the company's overall risk management system. The Board will, therefore, approve this Policy and any amendments thereto from time to time.

## ANNEXURE A

### I. Impact Scale

If the risks were to be realized, situations are then judged to evaluate, what would be the most likely outcome. The limits can be reviewed and proposed by the CRO to Executive Committee and Audit Committee for further inputs / revision at such periodic intervals as is considered necessary. The approval will be given by Body.

Risk Impact Scale							
Score	Rating	Financial			Reputational	Operations	Compliance
		Impact on Revenue	Impact on Profit (PBT)	Disclosure			
3	High	> 2.5% of Annual Turnover	> 5% of Annual Profit	<ul style="list-style-type: none"> <li>▶ Financial Statement Restatement / Material Misstatement</li> <li>▶ Instance of fraud leading to loss &gt; INR 5 Lakh</li> </ul>	<ul style="list-style-type: none"> <li>▶ Adverse publicity/ reputation damage to national &amp; state audience</li> <li>▶ Loss of confidence of 1 or more stakeholders</li> </ul>	<ul style="list-style-type: none"> <li>▶ Cessation or break down of operations in manufacturing unit (Cumulative &gt;7 days in any unit during the year)</li> <li>▶ Lack of safety measures leading to death of 1 or more individual or permanent disablement of more than 5 individuals during the year</li> <li>▶ Loss / disruption in IT systems leading to severe or ongoing business disruption (over 5 days during the year)</li> </ul>	<ul style="list-style-type: none"> <li>▶ Any failure to renew / obtain license / clearances impacting operations along with criminal liabilities on senior management</li> <li>▶ Large scale class action suit/case with implication of more than INR 5 Lakh</li> <li>▶ Any non-compliance leading to demand/payment of fines / penalties/ interests more than INR 2.5 Lakh</li> <li>▶ Any non-compliance leading to Regulatory investigation / scrutiny / vigilance by government agency</li> </ul>
2	Medium	> 1% of Annual Turnover and <= 2.5%	>2% of Annual Profit and <= 5%	<ul style="list-style-type: none"> <li>▶ Instance of fraud leading to loss up to INR 5 Lakh</li> </ul>	<ul style="list-style-type: none"> <li>▶ Adverse publicity/ reputation damage to local audience</li> <li>▶ Dissatisfaction in 3 or more stakeholder groups</li> </ul>	<ul style="list-style-type: none"> <li>▶ Cessation or break down of operations in manufacturing unit (Cumulative 4-7 days in any unit during the year)</li> <li>▶ Lack of safety measures leading to permanent disablement of 1 to 5 individuals or significant injury to more than 3 individuals during the year</li> <li>▶ Loss / disruption in IT systems leading to business disruption (more than 1 day but up to 5 days during the year)</li> </ul>	<ul style="list-style-type: none"> <li>▶ Any failure to renew/obtain license/clearances impacting operations</li> <li>▶ Large scale class action suit/case with implication of &gt; INR 2.5 Lakh up to INR 5 Lakh</li> <li>▶ Any non-compliance leading to demand/payment of fines/ penalties/ interests more than INR 1 Lakh up to INR 2.5 Lakh</li> </ul>
1	Low	Up to 1% of Annual Turnover	Up to 2% of Annual Profit	--	<ul style="list-style-type: none"> <li>▶ Limited damage to reputation</li> <li>▶ Dissatisfaction in less than 3 stakeholder groups</li> </ul>	<ul style="list-style-type: none"> <li>▶ Cessation or break down of operations in manufacturing unit. (Cumulative 1-3 days in any unit during the year)</li> <li>▶ Lack of safety measures leading to significant injury to 1 to 3 individuals during the year</li> <li>▶ Loss or disruption to systems leading to significant business disruption (up to 1 day during the year)</li> </ul>	<ul style="list-style-type: none"> <li>▶ Large scale class action suit/case with implication of up to INR 2.5 Lakh</li> <li>▶ Any non-compliance leading to demand/payment of fines/ penalties/ interests up to INR 1 Lakh</li> </ul>

## II. Likelihood Scale

The risk likelihood scale defines parameters for agreed upon timeframes over which risks may occur.

Risk Rating Criteria: Likelihood Matrix			
SCORE	RATING	Probability/Likelihood of the risk to occur and lead to assessed impact/consequence	
		Occurrence in future	Occurrence in the past
3	Expected/ Almost certain	Very high, will be almost a routine feature every month/quarter within the immediate next 12 months.	Similar instances have commonly occurred every quarter in the past 12 months.
2	Likely	High, may arise several times within the next 12 months.	Similar instances have occurred several times in the past 24 months
1	Unlikely	May occur once or twice in next 3 years.	There have been 1-2 similar instances in the past 3 years

The scale/matrix to be considered into taking all the 3 criteria or either one of them

**Inherent risk** is the risk that an activity would pose if *no controls* or other mitigating factors were in place i.e. the exposure arising from a specific risk before any action has been taken to manage it.

Risk Rating Matrix			
Likelihood	Impact/ Consequence		
	Low	Medium	High
Expected/Almost Certain	3	6	9
Likely	2	4	6
Unlikely	1	2	3