tbo.com
TRAVEL SIMPLIFIED

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 ("**Act**"), this Risk Assessment and Management Policy ("**Policy**") establishes the philosophy of TBO Tek 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 also 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.

Accordingly, the board of directors of Company ("**Board**") has adopted this Policy at its meeting held on November 24, 2021 which shall be applicable on and from November 24, 2021.

2. 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 assisting the Company in achieving its objectives safely. The objectives of the Policy can be summarized as follows:

(a) To safeguard the interests of the Company and / or it subsidiary(ies);

(b) To manage risks with an institutionalized framework;

(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.

3. 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.

4. Risk Management Committee

The Risk Management Committee ("**RMC**") shall have minimum of 3 (Three) members with majority of them being members of the Board of Directors, including at least 1 (One) independent director.

The chairperson of the RMC shall be a member of the Board of Directors and senior executives of the Company may be members of the Risk Management Committee.

The RMC shall meet at least twice in a year. The quorum for a meeting of the RMC shall be either 2 (Two) members or one-third of the members of the RMC, whichever is higher, including at least 1 (One) member of the Board of Directors in attendance.

The meetings of the RMC shall be conducted in such a manner that on a continuous basis not more than 180 (One Hundred and Eighty) days shall lapse between any two consecutive meetings of the Risk Management Committee.

5. Risk Management Framework

Conscious that no entrepreneurial activity can be undertaken without assumption of risks and associated reward 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.

A broad outline of the risk management framework is as under:

(a) Risk Identification: The management of the Company identifies potential events that may positively or negatively affect the Company's ability to implement its strategy and achieve its objectives and performance goals. Risks may be classified into two broad categories, namely internal risks and external risks. An illustrative list of such risks are as follows:

(i) Internal Risks:

- Strategic Risk: Competition, inadequate capacity, high dependence on a single customer/vendor.
- Business Risk: Project viability, process risk, technology obsolescence/ changes, development of alternative products.
- Finance Risk: Liquidity, credit, currency fluctuation.
- Environment Risk: Non-compliant with applicable environmental regulations, risk of health to people at large.
- Personnel Risk: Health & safety, high attrition rate, incompetence.
- Operational Risk: Process bottlenecks, non-adherence to process parameters/ pre-defined rules, fraud risk.
- Reputation Risk: Brand impairment, product liabilities.
- Regulatory Risk: Non-compliance to statutes, change of regulations.
- Technology Risk: Innovation and obsolescence.
- Information and Cyber Security Risk: Cyber security related threats and attacks, Data privacy and data availability.

(ii) External Risks:

- Sectoral Risk: Unfavourable consumer behaviour in relation to the relevant sector etc.
- Sustainability Risk: Environmental, social and governance relates risks.
- Political Risk: Changes in the political environment, regulation/ de-regulation due to changes in political environment.

(b) Root Cause Analysis: A root cause analysis shall be undertaken on a consultative basis. A root cause analysis enables tracing the reasons / drivers for existence of a risk element and helps developing appropriate mitigation action.

(c) Risk Scoring: The management of the Company considers qualitative and quantitative methods to evaluate the likelihood and impact of identified risk elements. The 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 revenue, profit, balance sheet, reputation, business and system availability etc. should the risk element materialize. The composite score of impact and likelihood are tabulated in an orderly fashion. The Company has assigned quantifiable values to each risk element based on the "impact" and "likelihood" of the occurrence of the risk on a scale of 1 to 4 as follows.

Impact	Score	Likelihood
Minor	1	Low
Moderate	2	Medium
High	3	High
Critical	4	Certain

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

(d) Risk Categorisation: The identified risks are further grouped in to (i) preventable; (ii) strategic; and (iii) 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. The management 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 Prioritisation: Based on the composite scores, risks are prioritized for mitigation actions and reporting.

(f) Risk Mitigation Plan: The 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. This risk mitigation plan drives policy development as regards risk ownership, control environment timelines, standard operating procedure, etc. The 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 may also cover (x) preventive controls - responses to stop undesirable transactions, events, errors or incidents occurring; (y) detective controls - responses to promptly reveal undesirable transactions, events, errors or incidents so that appropriate action can be taken; and / or (z) 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) 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.

6. Responsibility for Risk Management

Responsibility Holder	Responsibilities
Board	The Company's risk management architecture is overseen by the Board and the policies to manage risks are approved by the Board. The Board's role includes the following:

	(a) Ensuring that the Company has proper risk management framework; (b) Defining the risk strategy, key areas of focus and risk appetite for the Company; (c) Approving various risk management policies including the code of conduct and ethics; and (d) Ensuring that the senior management of the Company takes necessary steps to identify, measure, monitor and control these risks.
Audit Committee	The Audit Committee of the Company assists the Board in carrying out its oversight responsibilities relating to the Company's (i) financial reporting process and disclosure of financial information in financial statements and other reporting practices; (ii) internal control; (iii) compliance with laws, regulations, and ethics; and (iv) financial and risk management policies. Its role includes the following: (a) Setting policies on internal control based on the Company's risk profile, its ability to manage the risks identified and the cost/ benefit of related controls; (b) Seeking regular assurance that the system of internal control is effective in managing risks in accordance with the Board's policies; (c) Ensuring that senior management of the Company monitors the effectiveness of internal control system; and (d) Helping in identifying risk, assessing the risk, policies / guidance notes to respond its risks and thereafter framing policies for control and monitoring.
RMC	The RMC, as constituted by the Board, is the committee which implements and coordinates the risk function as outlined in this Policy on an ongoing basis. Its role includes the following: (a) Ensuring that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company; (b) Monitoring and overseeing implementation of this Policy, including evaluating the adequacy of risk management systems; (c) Conducting periodical review of this Policy, which shall be at least once in 2 (Two) years, while considering the changing industry dynamics and evolving complexity, and recommend for any amendment or modification thereof, as necessary;

	(d) Keeping the Board informed about the nature and content of its discussions, recommendations and actions to be taken; (e) Reviewing the appointment, removal and terms of remuneration of the Chief Risk Officer (if so appointed); (f) To implement and monitor policies and/or processes for ensuring cyber security; and (g) 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 laws.

7. 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.

8. Amendment

Any change in the Policy shall be approved by the Board. The Board shall have the right to withdraw and/or amend any part of this Policy or the entire Policy, at any time, as it deems fit, or from time to time, and the decision of the Board in this respect shall be final and binding. Any subsequent amendment/modification in the Act or the rules framed thereunder or the SEBI Listing Regulations and/or any other laws in this regard shall automatically apply to this Policy.

9. Communication of this Policy

This Policy shall be posted on the website of the Company i.e. https://www.tbo.com.