Indo Thai Securities Limited
Regd. Office: Capital Tower, 2nd Floor, Plot Nos. 169A-171,
PU-4, Scheme No. 54, Indore (M.P.), 452010, Tel.: 0731-4255800
E-mail: indothaigroup@indothai.co.in, CIN: L6610MP1995PLC008959

RISK MANAGEMENT POLICY

Table of Content

S. No	Table of Contents
1.	Background
2.	Objective
3.	Definitions
4.	Applicability
5.	Constitution Of Risk Management Committee
6.	Development Of Action Plan
7.	Risk Management Governance Structure
8.	Stakeholder Key Roles & Responsibilities
9.	Risk Management Procedures
10.	Risk Parameter Control For Trading
11.	Amendment

1. BACKGROUND:

The policy forms part of Indo Thai Securities Limited's ("Indo Thai" / "The Company") Internal control & Governance requirements. Also this Policy is in compliance with SEBI (Listing Obligations & Disclosure Requirements), Regulations, 2015 and provisions of Companies Act, 2013 read with Rules made thereunder which requires the Company to implement risk management system. Indo Thai Securities Limited recognizes that risk management is an integral part of good management practice. The policy explain Indo Thai approach to risk management, documents the roles & responsibilities of the Board, Audit Committee, Risk Management Committee, Risk Officers and Risk Owners etc. It also outlines the key aspects of the risk management process. This policy shall operate in conjunction with other business and operating / administrative practices.

2. OBJECTIVE:

The objective of the Risk Management Policy of the Company is to create and protect shareholder value by minimizing threats or losses, and identifying and maximizing opportunities. This Risk Management Policy is being applied in order to ensure that effective management of risks is an integral part of every employee's job. These include:

a) formulation and implementation of a comprehensive integrated risk assessment, governance, and management policy framework Providing a framework, that enables all the current and future risk exposure activities in a consistent and controlled manner with adequate systems of risk management and to identify internal and external risks faced by the Company including financial, operational, sectorial, sustainability, information, cyber security risks or any other risk as may be identified;
b) Improving decision making, planning and prioritization by comprehensive and structured understanding of business activities, volatility and opportunities/ threats;
c) Contributing towards more efficient use/ allocation of the resources within the organization;
d) Protecting and enhancing assets and Company's image;
e) addressing the root cause of the risks and to prevent recurrence of such risks by Preparing risk mitigation plans by setting up systems and processes for internal control of identified risks;
f) enable early identification and prevention of risk;
g) Reducing volatility in various areas of the business by developing and supporting people and knowledge base of the organization;
h) Optimizing operational efficiency by anticipating and responding to the changing economic, social, political, technological, legal and environmental conditions in the external environment;
i) Assess the likely impact of a probable risk event on various aspects of the functioning of the QSB such as impact on investors, financial loss to the QSB, impact on other

stakeholders in the market, reputational loss etc. and lay down measures to minimize the impact of such event;

j) Assign accountability and responsibility of Key Managerial Personnel (KMP) in the organization.

3. DEFINITIONS:

"Audit Committee" means Committee of Board of Directors of the Company constituted under the provisions of the Companies Act, 2013 and Regulation 18 of SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015

"Board of Directors" or "Board" in relation to a Company, means the collective body of Directors of the Company. [Section 2(10) of the Companies Act, 2013]

"Company" means "Indo Thai Securities Limited, a company constituted under the provisions of Companies Act, 2013.

"Risk Management Committee" means Committee of Board of Directors of the Company constituted under the provisions of the Companies Act, 2013 and Regulation 21 of SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015.

"Policy" means Risk Management Policy.

4. APPLICABILITY:

The Risk Management Policy shall come into force on and from 8th May, 2026.

5. CONSTITUTION OF RISK MANAGEMENT COMMITTEE:

Risk Management Committee shall be constituted by the Board, as and when required under the applicable law, consisting of such number of directors (executive or non-executive or independent directors) and such other officials like the Key Managerial Personnel (KMP) of the Company or any other persons as the Board thinks fit.

The Board shall define the roles and responsibilities of the Risk Management Committee and may delegate following activities to them:

a) to ensure that appropriate methodology, processes and systems are in place to manage and monitor and evaluate the implementation of action plans developed to address material business risks within the Company and its business units, and regularly reviewing the progress of action plans;

b) setting up internal processes and systems to control the implementation of action plans;
c) regularly monitoring and evaluating the performance of management in managing risk;
d) providing management and employees with the necessary tools and resources to identify and manage risks;
e) regularly reviewing and updating the current list of material business risks;
f) regularly reporting to the Board on the status of material business risks and the nature and content of its discussions, recommendations and actions to be taken;
g) review and monitor cyber security; and
h) ensuring compliance with regulatory requirements and best practices with respect to risk management
i) to periodically review the risk management policy, at least once in every year, including by considering the changing industry dynamics and evolving complexity.
j) the appointment, removal and terms of remuneration of the Chief Risk Officer (if any) shall be subject to review by the Risk Management Committee.

6. DEVELOPMENT OF ACTION PLAN:

The Board shall constitute a Risk Management Committee consisting of the following members and defined the Committee's role and responsibility: -

1. Mr. Parasmal Doshi
2. Mr. Dharmendra Jain
3. Mr. Amber Chaurasia
4. Ms. Shruti Sikarwar (As Secretary to the Committee)

The Committee shall not only assist in implementation of the Risk Management Plan of the Board but also monitor its implementation and review.

7. RISK MANAGEMENT GOVERNANCE STRUCTURE:

The organization structure and hierarchy of the Risk Management function is as under:

In the organization, respective functional head is responsible for managing risk arising in his/ her area of operations and the functional department is the primary owner of risks associated with that department.

Each department of the Company is required to formulate and implement Standard Operating Procedures, Guidelines, Templates, Processes, Catalogues, Checklists and Measurement Metrics for their respective functions/department.

The specific roles and responsibilities of various individuals/ bodies in the Risk Management hierarchy are indicated below.

8. STAKEHOLDER KEY ROLES & RESPONSIBILITIES:

Board of Directors

- The Board of Directors has the ultimate responsibility for managing the risk profile of the Organisation
- The Board shall constitute a Risk Management Committee with delegated powers from the Board.

Risk Management Committee

- To review the Risk Management Framework and undertake risk mitigation measures from time to time.
- To approve and recommend the Risk Management Policy which is to be placed in Board Meeting of the Company.
- The Risk Management Committee shall monitor implementation of the Risk Management Policy and keep the Board informed about its implementation and deviation, if any.
- To review the Risk Management Policy on half yearly basis and submit a report in this regard to the Stock Exchange.

Risk Management Department/Risk Officer

- Create a robust Risk Framework and ensure periodical reviews to keep it relevant with current goals and objectives of the Organization and abreast with the regulatory guidelines as may be issued from time to time.
- Lead and manage the Risk Management function holistically.
- Apprise the Risk Management Committee about all updates made to the Risk Management Framework during the half year including updates based on regulatory changes.
- Report on the risk assessment undertaken on an annual basis to be placed before the Risk Management Committee and observations and ensure remarks of the Committee on the risk assessment to be incorporated in the Minutes of Meeting

9. RISK MANAGEMENT PROCEDURES:

The stages of Risk Management process are as follows:

a. Risk Identification

This stage entails identifying risk factors, impact areas, events, their causes, and any potential repercussions. The possible event could have a beneficial or negative impact

on the company's goals. A variety of strategies are available to the organization for detecting uncertainties that could have an impact on one or more objectives. Following are some points which should be considered -

1. causes and events.
2. threats and opportunities.
3. vulnerabilities and capabilities.
4. changes in the external and internal context.
5. indicators of emerging risks.
6. consequences and their impact on objectives etc.
7. limitations of knowledge and reliability of information.
8. time-related factors.

Risks must be recorded in a Risk Register that includes details like the risk description, category, categorization, mitigation strategy, and relevant function or department.

b. Risk Analysis

The possibility of each risk happening, and its potential effects are determined through risk analysis. Each detected risk must be evaluated based on two criteria: the impact of an event's occurrence and the likelihood that it will occur. The level of risk exposure is produced by the combination of these two variables.

The potential impact may include -

- Operational impact (People / Technology / Operation)
- Reputational loss
- Regulatory repercussions
- Financial loss.
- Data Security and Privacy
- Legal

The number of prior occurrences in the industry, the audit findings from the prior year, anticipated future trends, or existing research shall be used to rate the risk's likelihood of occurrence (frequency).

Risks must be evaluated to determine the current degree of risk after taking into consideration the controls already in place. Each risk will be rated as Critical, High, Medium, or Low based on the assessments of the risks as per Risk Assessment Criteria.

This is further sub divided as mentioned below-

Assess **Inherent risks** – The risks at inherent level are evaluated assuming there is no control in place.

Assess **Residual risks** – The risks at residual level are evaluated factoring in the controls in place.

c. Risk Evaluation

"**Risk evaluation**" involves the comparison of the "risk severity" generated during the "risk analysis stage" with the risk criterion scale (created for both the likelihood and consequence) to determine if any additional action is required.

There could be different decisions which are taken at this level-

- Do nothing further.
- Consider risk treatment options.
- Undertake further analysis to better understand the risk.
- Manage and monitor existing controls.
- Reconsider objectives.

d. Risk Treatment

The risk treatment is a response to the risk evaluation. While doing risk treatment, it is understood that additional mitigation is needed to reduce the residual risk to a manageable level.

The risk treatment strategies listed below can be used to manage the risk's residual exposure. The best course of action must be chosen by weighing the benefits of additional risk mitigation against the costs, effort, or disadvantages of implementation. It may happen that the additional risk treatment strategy is not feasible in some circumstances; in such a case, the residual risk may need to be accepted and communicated.

Risk avoidance	By not performing an activity that could carry risk. Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed.
Risk transfer	Mitigation by having another party to accept the risk, either partial or total, typically by contract or by hedging / insurance.
Risk reduction	Employing methods/solutions that reduce the severity of the loss.
Risk retention	Accepting the loss when it occurs. Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater than the total losses sustained. All risks that are not avoided or transferred shall be retained by default.

e. Risk Monitoring and Reporting

To ensure that risks are kept within a reasonable range and that treatment measures have been taken and are working, monitoring of risks and treatment activities should be done on a frequent basis. A planned component of the risk management process with clearly defined roles should include ongoing monitoring and periodic reviews of the risk management process and its outcomes. Successful risk management depends on monitoring and review, thus it's important to specify who is in responsibility of carrying out these tasks.
The monitoring and review's findings and observations are most helpful when they are well-documented and disseminated.
In circumstances where the accepted risk of a particular course of action cannot be adequately mitigated, such risk shall form part of the consolidated risk register along with the business justification and their status shall be continuously monitored and periodically presented to the Risk Management Committee.

10. RISK PARAMETER CONTROL FOR TRADING:

- The system should allow only authorized users to set the risk parameter. Any change in Risk parameter should be well documented and changes should be done only by Authorised User with proper validation/re- confirmation.
- All the changes should be done through the following process:
  a) Proposal: All system changes must first be proposed by the software vendor.
  b) Approval: The proposed changes require approval from the System Administrator before implementation.
  c) Implementation: Upon approval, the changes will be executed by the authorized user.
  d) Audit & Compliance: A tamper-proof log must be maintained to record all changes for transparency and security.
- Risk Management System allows only those orders that are within the parameters as specified under this system.
- Risk Management System Should Consist of provisions for setting trading limits, exposure limits, position limits, order quantity limits order value limits, price range checks, Net Position limits for all CTCL / AT users based on risk assessment, credit quality and available margins of the client. Also appropriate limits for securities which are subject to FII limits as specified as RBI.

11. AMENDMENT:

The policy shall also be uploaded on the website of the Company at https://indothai.co.in/ .

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.

*****