



GENERIC ENGINEERING CONSTRUCTION AND PROJECTS LIMITED

# Risk Management Policy

INDEX OF CONTENTS :

Sr. No	Particulars	Page nos.
1.	Preamble	3
2	Definition	3-4
3	Object of the policy	4
5	Committee	5-6
6	Policy	6-12

## 1. PREAMBLE

The Securities and Exchange Board of India (“the “SEBI”) has notified Second Amendment in the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 (“SEBI LODR Regulations”) w.e.f. 5.5.2021. as per regulation 21 of the SEBI LODR Regulations mandates every top 1000 listed entities (determined on the basis of market capitalisation as at the end of the immediate previous financial year) and as per Regulation 17 of the SEBI LODR Regulations, the board of directors shall be responsible for framing, implementing and monitoring the risk management plan for the listed entity.

Furthermore, in accordance with Section 134(3)(n) of the Companies Act, 2013, a company is required to include a statement indicating development and implementation of a risk management policy for the company including identification therein of elements of risk, if any, which in the opinion of the Board may threaten the existence of the company in the directors report of the company.

Accordingly, to mitigate and manage risk at “The Investment Trust of India” (hereinafter referred to as the “Company”), the Company has formed the policy (the “Risk Management Policy”) for the same.

This document shall be under the authority of the Board of Directors of the Company. It seeks to identify risks inherent in the operations of the Company and provides guidelines to define, measure, report, control and mitigate the identified risks.

## 2. DEFINITION

- a) "Board of Directors" or “Board” in relation to the Company, means the collective Body of Directors of the Company (including a committee of directors of the Company duly authorized by the Board).
- b) “Company” means “The Investment Trust of India”, a company constituted under the provisions of Companies Act, 1956.
- c) Control :- Controls are defined as the power to influence or direct people’s behavior or the course of risk events.
- d) Committee means Risk Management Committee constituted or reconstituted by the Board from time to time.
- e) "Policy" means this Risk Management Policy as may be amended or supplemented from time to time.
- f) Process would mean series of actions or steps taken to achieve an end. All processes individually and severally shall cover all business activities for each of the risk assessment function
- g) Risks are events or conditions that may occur, and whose occurrence, if it does take place, has a harmful or negative impact on the achievement of the organization’s business objectives. The exposure to the consequences of uncertainty constitutes a risk.
- h) Risk Management is the process of systematically identifying, quantifying, mitigating and managing all risks and opportunities that can affect achievement of a corporation’s strategic and financial goals.

- i) Risk Event / Trigger Point can be defined as a discreet occurrence that negatively affects strategy, decision and process and results in a pecuniary loss.
- j) The Risk Strategy of a company defines the company's standpoint towards dealing with various risks associated with the business. It includes the company's decision on the risk tolerance levels, and acceptance, avoidance or transfer of risks faced by the company.
- k) Risk Assessment is defined as the overall process of risk identification, assessment, risk prioritization and execution of appropriate response strategy to ensure that effective and efficient controls or risk mitigation activities are in place to address potentially high- impact operational risks and take necessary steps to ensure that they are sustainable over a period of time.
- l) Risk Estimation is the process of quantification of risks.
- m) Response Strategy  
These are a set of activities that will determine the follow-up measures that will be undertaken by the Risk assessment committee to mitigate the risk.
- n) Likelihood is the probability or frequency of risk event occurring at any given period of time.

### 3. OBJECTIVES OF THE POLICY

The main objective of this policy is to ensure sustainable business growth with stability and to promote a proactive approach in reporting, evaluating and resolving risks associated with the business. In order to achieve the key objective, the policy establishes a structured and disciplined approach to Risk Management, including the development of the Risk Matrix, in order to guide decisions on risk related issues. The specific objectives of the Risk Management Policy are:

- a) To ensure that all the current and future material risk exposures of the company are identified, assessed, quantified, appropriately mitigated and managed
- b) To establish a framework for the company's risk management process and to ensure companywide implementation
- c) To enable compliance with appropriate regulations, wherever applicable, through the adoption of best practices
- d) To assure business growth with financial stability
- e) To monitor and review the cyber security and related risks.

### 4. COMMITTEE

#### 1. COMPOSITION:

The Committee shall have minimum three members with majority of them being members of the board of directors, including at least one independent director.

The Company Secretary shall act as the Secretary to the Committee.

2. MEETINGS:

The Committee shall hold meeting as and when required, to discuss various issues on implementation of the Policy of the Company. However committee shall meet at least twice in a year and gap between two meetings shall not be more than one hundred and eighty days. The members would thrive to attend all the meetings held in a financial year.

3. QUORUM:

The quorum for a meeting of the Risk Management Committee shall be either two members or one third of the members of the committee, whichever is higher, including at least one member of the board of directors in attendance.

4. Roles of the Committee:

1) To formulate a detailed risk management policy which shall include:

(a) A framework for identification of internal and external risks specifically faced by the Company, in particular including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk as may be determined by the Committee.

(b) Measures for risk mitigation including systems and processes for internal control of identified risks.

(c) Business continuity plan.

2) To ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company;

3) To monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems;

4) To periodically review the risk management policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity;

5) To keep the board of directors informed about the nature and content of its discussions, recommendations and actions to be taken;

6) The appointment, removal and terms of remuneration of the Chief Risk Officer (if any) shall be subject to review by the Committee.

7) The Risk Management Committee have powers to seek information from any employee, obtain outside legal or other professional advice and secure attendance of outsiders with relevant expertise, if it considers necessary.

The Risk Management Committee shall coordinate its activities with other committees, in instances where there is any overlap with activities of such committees, as per the framework laid down by the board of directors.

## 5. POLICY

In order to fulfil the objectives of this policy and lay a strong foundation for the development of an integrated risk management framework, the policy outlines the following guiding principles of Risk Management:

## Principles of Risk Management

1. All business decisions will be made with the prior information and acceptance of risk involved.
2. The Risk Management Policy shall provide for the enhancement and protection of business value from uncertainties and consequent losses.
3. All employees of the company shall be made aware of risks in their respective domains and their mitigation measures.
4. The risk mitigation measures adopted by the company shall be effective in the long- term and to the extent possible be embedded in the business processes of the Company.
5. Risk tolerance levels will be regularly reviewed and decided upon depending on the change in company's strategy.
6. The occurrence, progress and status of all risks will be promptly reported and appropriate actions be taken thereof.

## 6. Risk Management Policy Statement

The policy statement is as given below:

1. To ensure protection of shareholder value through the establishment of an integrated Risk Management Framework for identifying, assessing, mitigating, monitoring, evaluating and reporting of all risks.
2. To provide clear and strong basis for informed decision making at all levels of the Organisation.
3. To continually strive towards strengthening the Risk Management System through continuous learning and improvement.

## 7. Risk Governance Structure



## 8. Key Risk area's and trigger points

Impact	Parameter	1	2	3	4	5
Area		Insignificant	Minor	Moderate	Major	Significant
Growth	Turnover growth standalone (TS) Compared with last 6months Turnover	If TS decrease by 1%	If TS decrease by 5%	If TS decrease by 10%	If TS decrease by 15%	If TS decrease by 20%
	Turnover growth Consolidated (TC) Compared with last 6months Turnover	If TC decrease by 1%	If TC decrease by 5%	If TC decrease by 10%	If TC decrease by 15%	If TC decrease by 20%
Trade	Average	Outstanding	Outstanding	Outstanding	Outstanding	Outstanding
Receivables at Group level	collection period of Trade receivables (outstanding from vendor)	more than 25 days on targeted trade receivables days	more than 25-30 days on targeted trade receivables days	more than 1-3 month on targeted trade receivables days	more than 3-6 months on targeted trade receivables days	more than 6 months on targeted trade receivables days
Trade Payables at Group level	Average payment period of Trade receivables (Outstanding payables)	Outstanding more than 25 days on targeted trade payable days	Outstanding more than 25-30 days on targeted trade payable days	Outstanding more than 1-3 month on targeted trade payable days	Outstanding more than 3-6 months on targeted trade payable days	Outstanding more than 6 months on targeted trade payable days

Gross profit	Gross profit standalone Compared with last 6months Turnover	If GP decrease by 1%	If GP decrease by 5%	If GP decrease by 10%	If GP decrease by 15%	If GP decrease by 20%
	Gross profit consolidation Compared with last 6months Turnover	If GP decrease by 1%	If GP decrease by 5%	If GP decrease by 10%	If GP decrease by 15%	If GP decrease by 20%
Compliance	Non-compliance to legal and regulatory requirement	Insignificant or no Impact	Warning show cause legal notice	Statutory Penalty upto Rs. 10 lakhs	Statutory Penalty above 10lakhs	Summon by any court to any officials
Failure of IT Set ups / Software License Compliances / Shut Down / Break Down -		No Halt in operations	Halt in operations for less Half a day	Halt in operations for less than a day	Halt in operations for more than a day	Halt in operations for more than Two days
Data Backup and Disaster Recovery System		Back up taken at regular intervals.	Back up taken periodically,	Back up taken Infrequently .	Back up is not taken	Back is not taken and loss of data
Email and Password Controls		Frequent changes in passwords	Password changed insignificantly	-	Passwords never Changed	Passwords never Changed and email got hacked
Virus Protection Measures		Up to date virus protection measures	-	Virus protection measures not updated	Weak Virus protection	Weak Virus protection and system got infected
Software Licenses Compliances		Strong Compliance s over	-	Less Compliance s towards	Weak Compliances over	Weak Compliance s



		Licenses		licenses	Licenses	over Licenses and notice received from license vendor
Server Room Infrastructure		Strong controls over Server Room Infrastructure	-	Server Room Infrastructure not up to date	Weak Controls over Server Room Infrastructure	Weak Controls over Server Room Infrastructure and loss of data saved in server
Human Resource	Employee Attritions	Attrition less than 5 % at key positions/skill levels	Attrition between 5-10 % key positions/skill levels	Attrition between 10-15% key positions/skill levels	Attrition between 15-20 %key positions/skill levels	Attrition more than 20 % key positions/skill levels

**Risk assessment:-** The risk owners will do the risk assessment on quarterly basis and submit the risk assessment report (RAR) to Chief Risk Officer (CRO) and CRO will submit the report to Risk Management committee and decide the risk mitigation plans, if requires.\

Further, if RAR is more than 3 (Moderate) then Risk management committee will submit the report along with the risk mitigation plans to Audit committee and Board.

Audit committee and Board will review the risk mitigation plans submitted by the Risk management committee and approves the same with or without changes.

## 9. Types of Risk affecting the Company

Recognizing the kind of risks that Company is/may be exposed to, risks will be classified broadly into the following categories:

1. Strategic Risk: include the range of external events and trends (like Government policy, competition, Political and economical instability, Market Dynamism, International economy, Foreign Currency risk) that can adversely impact the Company's strategic growth trajectory and destroy shareholder value.

2. Business Risk: include the risks associated specifically with the Company and having an adverse impact on the company's capability to execute activities critical for business growth, thereby affecting its near-term performance. Business Risk includes;
  - a) Concentration risk  
It is defined as probability of loss arising from heavily lopsided exposure to a particular group of counterparties.
  - b) Competition risk  
It is defined as probability of loss from decline in a firm's competitiveness on account of rivalry.
  - c) International operations risk  
  
The inherent risks in conducting business internationally include: i - country-risk or the risk of the region that we operate in, changes in politico-economic conditions, laws, or regulatory requirements.  
ii- Country-specific tax obligations. iii- Trade barriers and import/export licensing requirements.
3. Operational Risk: are those risks which are associated with operational uncertainties, like
  1. Risks arising for failures to comply with operational policies and procedures on a daily basis, e.g. maintenance, supplier selection, quality, etc.
  2. Risks arising from variations in the quality and availability of the Company's personnel, e.g. recruitment, training, remuneration, development, etc.
  3. Risks associated with computer and communications hardware, software and data, e.g. obsolescence, security, availability, access, back-up, etc.
4. Force Majeure events like floods affecting operations, theft of key equipment and other acts of God.
5. Commodity risk  
Factors that can affect commodity prices include political and regulatory changes, seasonal variations, weather, technology and market conditions. Commodity price risk is often hedged by major consumers. Unexpected changes in commodity prices can reduce a producer's profit margin, and make budgeting difficult. Futures and options are two financial instruments commonly used to hedge against commodity price risk.
6. Compliance risk  
Compliance risks are those associated with the need to comply with laws and regulations. They also apply to the need to act in a manner which investors and customers expect, for example, by ensuring proper corporate governance. Risks arising from non-compliance with existing laws and regulations or the potential adverse impact of a change in rules and regulations, e.g. Health & Safety, Environmental, Labour Laws, Food & Safety Laws, Drugs, Concession and Permit requirements, etc.
7. Financial risk, for example non-payment by a customer or increased interest charges on a business loan, risks arising from failure to manage financial aspects, e.g. credit (customers), liquidity (availability of

cash) and market risk exposures (foreign and commodity price fluctuations) and to provide complete, accurate and meaningful financial reports for internal and external users. Financial Risk includes:

a) Credit risk

It is defined as probability of loss arising from a Debtor's default on account of non- payment of financial consideration.

b) Treasury/foreign exchange risk

It is defined as probability of loss occurring from an adverse movement in foreign exchange rate.

8. Environmental risks, including pollution control measures of the Government. The potential for adverse effects and damage on living organisms/human life associated with pollution of the environment by effluents, emissions, wastes, or accidental chemical releases; energy use; or the depletion of natural resources.
9. Health and safety risks includes risk of food adulteration, pandemic, accident/Incident that results in injury, illness, disease, damage or loss at workplace.
10. Business development risk includes failure of business strategies, product diversification, marketing strategies, competition, etc.
11. Market risk includes changes in share price of the Company, BVPS, PE Ratio and other financial ratios.
12. Risk of Unutilized Capacity: One of the important segments of the Company is solvent extraction is highly affected by seasonal factors. So there are chances of financial losses in months in which there are no operations and lower production due to lack of orders.
13. Product Liability Risk includes liability on Company on account of supply of low /bad quality products.
14. Risks related to Financial Reporting / Ineffective Controls includes non-compliance of Accounting Standard issued by the ICAI, Accruals not reversed in the beginning of the next period, Reconciliation of balance sheet not prepared etc. resulting in misstatement in financial statements, Ineffective Controls resulting in frauds, errors, non-compliance of laws / Company policies.

## 10. Risk Mitigation/ Risk Management Process

The risk mitigation can be planned using the following key strategies:

- a) 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.
- b) Risk Transfer: Mitigation by having another party to accept the risk, either partial or total, typically by contract or by hedging.

- c) Risk Reduction: Employing methods/solutions that reduce the severity of the loss
- d) 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 over time than the total losses sustained. All risks that are not avoided or transferred are retained by default.

#### 11. Risk Management Process:

The process of managing the Risk includes the following:

1. Identify the Risks: Risks in the company are identified through 1) inquiries to management and other senior personnel 2) Observation/inspection and 3) By performing analytical procedures.
  - a) Inquiries are done regarding their operating style, incentive plans, budgets etc.
  - b) Inspection is done for business plans / strategies, internal controls, reports available in accounting software, minutes etc.
  - c) Analytical procedures include comparing trends, growth and other quantitative data related to key risks.

2. Evaluating and assessing the Risks: Risks are evaluated keeping in consideration their significance and likelihood of occurrence. Significance is assessed by the impact of it on profit / compliance / governance. Likelihood is judged by viewing the historic events of the occurrence of such risks and probability of its occurrence taking into consideration the weakness of internal controls leading to its frequency of occurrence.

Accordingly, the risks identified are categorized in Low / Medium / High.

3. Handling/Controlling the Risks by-- - Risk Prevention,
  - Risk Avoidance,
  - Risk Transfer,
  - Risk Retention and - Risk Control.
5. Monitoring/Reporting
6. Risk Management Policy and implementation.

Objectives shall be set at the strategic level, establishing a basis for operations, reporting and compliance objectives. Identifying the most relevant risks based on situation, evaluate the level of risks based on probability and the significance of their potential impact. Decide appropriate management action to respond to assessed risk. Monitor the implementation and success of risk mitigation action plan. Report to the appropriate level to meet reporting requirements.

#### 12. Risk Adjustment, Management and Minimization Procedure:

Actions to reduce the likelihood or impact by transfer the full or portion of the risk, e.g. hedging, insurance for fires, insurance for Directors and Officers liability cover, etc.

### 13. Subsidiary/group companies

Subsidiary/group companies Subsidiary/group companies shall formulate there risk management policy based on this policy and may add more risk as applicable to specific industry or are of operation.