ANANDRATHI
Private Wealth. uncomplicated

Anand Rathi Wealth Limited

Risk Management Policy

(Amended as on 06th January, 2024)

Reviewing Authority	Risk Management Committee
Approving Authority:	Board of Directors
Original Issue Date:	16th July 2021
Last Review Date:	20th March, 2023 & 11th July, 2023
Current Review Date:	06th January, 2024
Version No.:	1.5
Review Cycle:	At such Intervals as prescribed under SEBI (Listing Obligation and Disclosure Requirement) Regulation, 2015.
Applicability	Anand Rathi Wealth Limited and its Subsidiaries

Risk Management Committee Charter

Contents

1. Purpose and Objectives

1. The Risk Management Committee ("Committee") is a committee which has powers delegated to it by the Board of Directors ("Board") of Anand Rathi Wealth Limited ("Company") for overseeing and managing the organization's risk management activities.
2. The primary objectives of the Committee is that of assisting the Board in-
    - Overseeing and managing the organization's risk management activities,
    - Ensuring that effective risk management practices are in place to identify, assess, mitigate, and monitor risks within the Company,
    - Fulfilling its corporate governance oversight responsibilities regarding the identification, evaluation, and mitigation of operational, strategic, and external environmental risks,
    - Monitoring the Risk Management Policy and associated practices for governance purposes,
    - Safeguarding the organization's assets, reputation, and overall sustainability by providing guidance and oversight on risk-related matters,
    - Reviewing risk assessment of the Company annually and monitoring of various risks including credit risk, financial & operational risks, technology risk, market risk, liquidity risk, investment risk, cybersecurity risk, forex risk, commodity risk, etc,
    - Monitoring of the Company's risk tolerance, capital liquidity and funding.

2. Composition

1. The Composition of the Committee shall be in accordance with SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015. The Committee shall be chaired by the Member of the Board.
    - The Risk Management Committee shall have minimum three members with majority of them being members of the board of directors, including at least one independent director and in case of a listed entity having outstanding SR equity shares, at least two thirds of the Risk Management Committee shall comprise independent directors.
    - The Chairperson of the Risk management committee shall be a member of the board of directors and senior executives of the listed entity may be members of the committee.

3. Frequency of Meetings

1. The Committee shall meet on need basis and between the two meetings gap shall not be more than 180 days.

4. Notice of Meetings and Agenda

1. The notice of the meeting and its agenda shall be circulated by the Company Secretary at least 7 days prior to the date of the meeting to the Committee Members.
2. In case of any risks having an impact on the Company (financially or non – financially) which are considered in the Risk Register shall be included in the agenda.
3. The agenda items to be transacted at the meetings shall include but is not limited to:
    - Discussion on previous meeting action points.
    - Top Risks for the Company and mitigation measures for the same

- Presentation / Update from respective functional heads over the Top risk for respective function, Risk Indicator, Mitigation measures undertaken etc.
- Any other agenda as the Committee may deem appropriate.

5. Quorum

1. The quorum for the meeting of the Committee shall be any two members or one-third of the members of the Committee, whichever is greater, with at least one Independent Director being present.
2. The Committee Members may invite Company Executives and external consultants, as considered appropriate.
3. A duly convened meeting of the Committee at which the requisite quorum is present shall be competent to exercise all or any of the authorities, powers, and discretions vested in or exercisable by the Committee. The invitees other than the Committee members shall have the right to be heard in the Meetings, but they shall not have the right to vote.

6. Minutes of Meetings

1. The Company Secretary shall prepare the minutes of all meetings of the Committee and circulate the same within 15 (fifteen) days from the date of the conclusion of the meetings.

7. Roles and Responsibilities

1. Roles

i. To formulate a detailed Risk Management Policy, which shall include but is not limited to;
  - Framework for identification of internal and external risks specifically faced by the Company, including financial, operational, cybersecurity risks or any other risk as may be determined by the Committee.
  - Measures for risk mitigation, including systems and processes for internal control of identified risks.

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

iii. To monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems.

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

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

vi. 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.

2. Responsibilities

i. Review the Company's risk governance structure, risk assessment and risk management practices and guidelines, policies and procedures for risk assessment and risk management, including the risk management plan.

ii. Review and approve the Enterprise-wide Risk Management (ERM) framework.

iii. Review the alignment of the ERM framework with the strategy of the Company.

iv. Monitor the Company's risk appetite and strategy relating to key risks, including credit risk, liquidity and funding risk, market risk, cybersecurity risk, forex risk, commodity risk, product risk and reputational risk, as well as the guidelines, policies, and processes for monitoring and mitigating such risks.

v. Oversee Company's process and policies for determining risk tolerance, and review management's measurement and comparison of overall risk tolerance to established levels.

vi. Review and analyse risk exposure related to specific issues, concentrations, and limit excesses, and provide oversight of risk across the organization.

vii. Review compliance with risk policies, monitor breaches / trigger trips of risk tolerance limits and direct action.

viii. Nurture a healthy and independent risk management function in the Company.

ix. Update Audit Committee regarding top risks identified by the Management / Risk Management Committee and mitigation measures for each of the identified risks including way forward to prioritize and re-consider risk treatment strategy already defined.

x. Carry out any other function as is referred by the Board from time to time or enforced by any statutory notification / amendment or modification as may be applicable.

8. Review

1. The Committee shall review and assess the adequacy of the Charter annually and recommend the changes, if any, to the Board for their approval. Any change pertaining to the Charter will be reviewed and approved by the Board.

2. The Risk Management Committee shall make regular updates to the Board regarding Enterprise Risk Management.

ANAND RATHI WEALTH LIMITED

RISK MANAGEMENT PROCEDURE

In conjunction with

Risk Management Policy

Reviewing Authority	CXOs, Functional Heads of the Company
Approving Authority:	Risk Management Committee of the Company
Original Issue Date:	
Last Revision Date:	-
Version No.:	1.0
Review Cycle:	Every 6 months or change in policy whichever is earlier
Applicability	The Company and its Subsidiaries

INDEX

1. Preface - Enterprise Risk Management Procedure

- Enterprise risk management (ERM) is the process of planning, organizing, directing and controlling the activities of an organization to minimize the harmful effects of risk.
- ERM Program is a structured, consistent, and continuous process of measuring or assessing risk and developing strategies to manage risk within the risk tolerance levels.
- This document contains details of the Risk Management policy framework adapted by the Anand Rathi Wealth Limited.

2. Objectives

The objective of a Risk Management Procedure is to provide a structured and consistent approach in identifying, assessing, evaluating, mitigating, monitoring and reporting risks arises both due to internal and external environments. The Risk management procedure serves as a guide for all stakeholders w.r.t. robust implementation of Enterprise Risk Framework and ensuring that risk management processes are executed in a systematic and effective manner.

- Ensuring standardization of practices across the company for risk management (This covers all components of Risk Management cycle)
- Setting clear roles and responsibilities amongst Risk Owners, Risk Controller, CXOs / Functional Heads / Sr. Management thereby ensuring accountability and responsibility.
- Establish guidelines for documenting the Risk register and reporting risk management activities and outcomes to the Risk Management Committee
- Define the requirement for maintaining records, documenting risk assessments, and reporting risk-related information to the Risk Management Committee and promoting transparency & accountability.
- Implement a proactive approach to enhance risk awareness amongst stakeholders across the company and ensure that risks are not overlooked or underestimated. It guides stakeholders to consider a wide range of potential risks that may affect the organization's objectives.
- With documented procedures and guidelines, it promotes continuity in risk management efforts, even during absence of internal stakeholders.
- It serves as a valuable resource for learning from past experiences and improving risk management practices. It allows organizations to capture understanding gained from experience, update procedures based on feedback and emerging best practices, and continuously enhance their risk management capabilities.
- Define transparent procedure involving any changes in Risk Register and reporting of the same.
- Provide a guideline for risk analysis and calculate risk score.
- Provide a guideline for maintenance of Risk register.
- Provide a guideline for risk measurability, its impact assessment.

3. Scope

It encompasses all areas of the organization, including sales, operations, finance & accounts, human resources, information technology, legal, and strategic/business planning.

This document sets out the guidelines for below:

- Establishing the External Context and Internal Context for risk identification
- Identification of risks and steps to be followed in risk identification
- Addition and Modification of risks in Risk register
- Risk Assessment and Analysis
- Risk Treatment
- Risk Monitoring and Review
- Risk Reporting

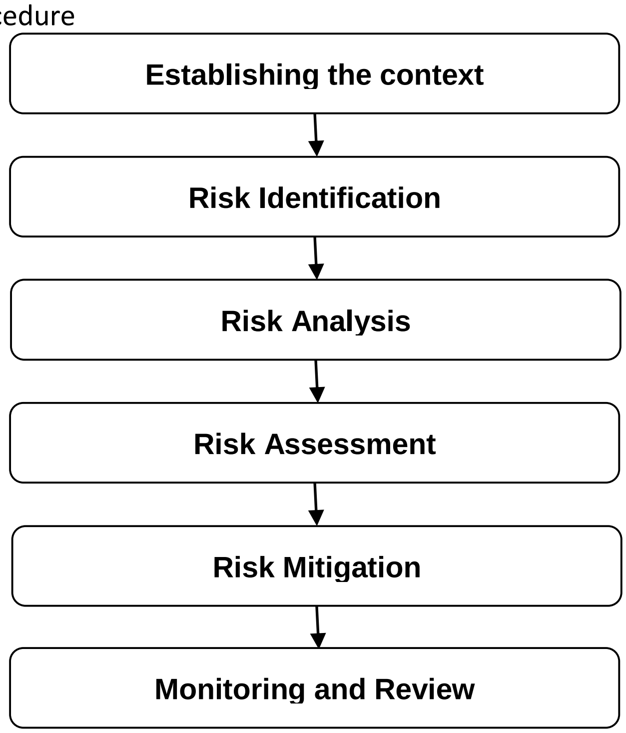
This document acts as standard operating procedure for adherence and compliance to Risk Management Framework.

4. Risk Management Procedure

The risk management system is dynamic and is designed to adapt to developments and any changes in the risk profile over time. Compliance measures are used as a tool to address identified risks.

The Risk Management Process is a clearly defined method of understanding what risks and opportunities are present, how they could affect a project or organization, and how to respond to them.

Summary of Procedure



The risk management system is based on a structured and systemic process which takes into account internal and external risks.

The main elements of the risk management process are as follows:

- Establishing the Context
- Risk Identification
- Risk Assessment (analysis & evaluation)
- Risk mitigation
- Monitoring and Review
- Risk Reporting

5. Establishing the Context

Define the objectives and identify the external and internal parameters to be considered while identifying and managing the risks. It sets the scope for the risk management process and also the criteria for which the risks will be assessed, along with key drivers and trends that have an impact on the objectives of the organization.

5.1. External Context

Understanding the external context is important to ensure that the objectives and concerns of all stakeholders are considered when developing risk criteria. It is based on the organization-wide context, but with specific details of legal and regulatory requirements, stakeholder perceptions and other aspects of risks specific to the scope of the risk management process.

The external context can include, but is not limited to:

- The social and cultural, political, legal, regulatory, volatility of the financial markets, technological, economic, natural and competitive environment, whether international, national, regional or local;
- Relationships with perceptions and values of all the stakeholders.

5.2. Internal Context

The risk management process is aligned with the organization's culture, processes, structure and strategy. Internal context is anything within the organization that can influence the way risks will be managed. Internal establishing context refers to the process of defining and understanding the internal factors and conditions within an organization that shape its risk management activities. It involves identifying and assessing elements such as organizational objectives, governance structure, policies and procedures, risk appetite, stakeholder expectations, internal resources, risk management roles and responsibilities, communication channels, and monitoring processes. Establishing context internally provides a clear understanding of the organization's internal environment and helps align risk management practices with its objectives, culture, and capabilities. It is necessary to understand the internal context. This can include, but is not limited to:

- Governance, organizational structure, roles and accountabilities;
- Policies, objectives, and the strategies that are in place to achieve them;
- Capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- The relationships with and perceptions and values of all the stakeholders;
- The organization's culture;
- Information systems, information flows and decision-making processes (both formal and informal);

6. Risk Identification

Risk identification is the process of systematically identifying potential risks or threats that could negatively impact the company. The goal is to identify and understand these risks so that appropriate measures can be taken to mitigate or manage them effectively.

6.1. Key steps and techniques used for risk identification:

- Review of Risk Register: Risk registers contain a list of common risks associated with the specific domain or industry. These checklists can help prompt ideas and ensure that no significant risks are overlooked.

- External sources: Keep track of external sources of risk information, such as industry reports, market trends, technological advancements, regulatory changes, and geopolitical factors that may impact the project or organization.

- Feedback, Past Learnings & Expert Judgement: Seek inputs from experts which help in early identification of events that may have a negative impact on organization, along with feedback from CXOs, stakeholders, and other relevant parties regarding potential risks they have encountered or foreseen. Also, review lessons learned from previous projects to identify recurring or common risks.

  As per above steps, risk identification is done mainly in meetings with CXOs, Functional Heads, Risk owners, Sr. Management

6.2. Identification of New Risk: -

- Any new risk identified is further discussed for below:

Particulars	Description
Classification of Risk	External Risk or Internal Risk
Type of Risk	E.g. Compliance Risk or Country Risk
Trigger of Risk	Events or circumstances that can activate or initiate the happening of a risk. E.g. Market Volatility

Cause of Risk	Causes of risks are the underlying factors or events that contribute to the occurrence or manifestation of a risk. E.g., Economic Recession
Impact of Risk	The impact of risk refers to the potential consequences or effects that an event can have on an organization. E.g., Loss of reputation, Financial & Liquidity risk, etc.
Mitigation measures	Mitigation measures refer to actions taken to reduce or prevent the adverse impacts of a particular event or phenomenon. Pre-Assessment of risk: Substantial financial losses due to economic recession or poor investment decision Post-Assessment of risk: Minimize financial losses by diversification of investment portfolios, through due diligence.

Based on consensus of Risk Controller and Functional Head/CXOs, new risk is added in Risk Register.

6.3. Changes in Existing Risk

Such modification can be made due to following factors For e.g. Anti-Money Laundering (AML) Risk

Particulars	Description
Trigger of Risk	Criminals and money launderers continuously adapt their tactics to evade detection. As new money laundering techniques emerge, such as the use of virtual currencies or prepaid cards, the trigger for AML risk may need to be updated to capture these activities.
Cause of Risk	Governments and regulatory bodies continuously update AML laws and regulations to address emerging threats and vulnerabilities. Changes in legislation, such as the implementation of new AML directives or regulations, can increase or decrease the causes of risk.

Impact of Risk	Non-compliance with AML regulations can lead to regulatory enforcement actions, including fines, sanctions, and restrictions on business operations. E.g., Pre-Mitigation: Financial losses due to paying non-compliance penalty or fines Post-Mitigation: Complying the regulations stated by legal authority can minimize financial loss.
Mitigation measures	If money launderers adapt new techniques for money laundering, then mitigation methods to be changed according to that.

Post change in above referred criteria, parameters are reviewed to analyze whether risk finds place in Risk Register or not.
Based on analysis, following action is taken :
A. If risk is to be included in Risk Register - Updated in Risk Register & changes to be reported to Risk Management Committee.
B. If risk is not included in Risk Register – Non-reported risks & changes should be reported to Risk Management Committee.

6.4. Updating the Risk Register

All the risks captured in Risk Register are reviewed and discussed by CXOs, Functional Head. Any change in either Internal environment or External environment which indicates either reduction in likelihood, minimal impact may direct re-consideration of risk already existing in Risk Register.

The analysis is conducted on below:

Particulars	Description
Trigger of Risk	Being updated about the changes in regulations can lead to reduction in trigger of risk.
Cause of Risk	Foster a culture of continuous improvement by learning from past experiences and adapting strategies based on lessons learned can reduce the cause of risk.
Impact of Risk	If the impact of risk is reduced due to adaptation of appropriate mitigation methods, then it can remove the risk from the Risk register. E.g. Implementing strong access controls and user authentication mechanisms.

7. Risk Register

7.1. Definition

A risk register is a document that is used as a risk management tool to identify potential setbacks within a project. This process aims to collectively identify, analyze, and solve risks before they become problems. While usually centered around projects, other circumstances where risk management is helpful include product launches. It serves as a central repository of information for managing and monitoring risks throughout their lifecycle. A project risk register should not only identify and analyze risks, but also provide tangible mitigation measures. This way, if the risk becomes a larger threat, your team is prepared with solutions and empowered to solve the issues.

7.2. Objectives of Risk Register

7.2.1 To facilitate centralized information
7.2.2 To provide risk visibility
7.2.3 Facilitates effective communication and collaboration among stakeholders.
7.2.4 Enables a proactive approach to identifying, analyzing, and mitigating risks.
7.2.5 Helps prioritize risks and allocate resources accordingly.
7.2.6 Supports compliance with regulatory requirements and internal governance standards
7.2.7 Promotes a culture of continuous improvement in risk management practices

8. Risk Assessment

Risk Assessment and Analysis is a vital component of risk management that involves assessing and understanding the nature, characteristics, and potential impact of identified risks. Analyze each identified risk to understand its characteristics, causes, and potential consequences. This includes assessing the likelihood of the risk occurring and the potential impact it may have on the organization or project objectives. Use quantitative and qualitative analysis techniques, such as probability and impact matrices, risk scoring, or scenario analysis.

Key steps in Risk assessment

- Identify and document all potential risks that may affect the organization or project. This step involves gathering information from various sources, such as historical data, expert knowledge, documentation, and stakeholder input.
- Develop a clear and concise description for each identified risk. Describe the risk event, it's causes and sources of risk, the trigger events that would lead to the occurrence of the risks, the positive and negative consequences of the risk and the likelihood that those consequences can occur.
- Establish criteria for assessing risks, including the likelihood of occurrence, Financial, Strategic, Reputational and Compliance impact. Define scales or categories to measure

the likelihood and impact levels consistently. These criteria can be qualitative (e.g., Low, Medium and High

Level of risk = consequence x likelihood

a) Likelihood scale example

Level	Likelihood	Description
4	Very likely	Happens more than once a year in the industry
3	Likely	Happens about once a year in the industry
2	Unlikely	Happens every 10 years or more in the industry
1	Very unlikely	Has only happened once in the industry

b) Consequences scale example

Level	Consequence	Description
4	Severe	Financial losses greater than Rs.10 Crores
3	High	Financial losses between Rs.5 Crores to Rs.10 Crores
2	Moderate	Financial losses between Rs.1 Crore to Rs.5 Crores
1	Low	Financial losses less than Rs.1 Crore

Note- Ratings vary for different types of businesses. The scale above uses 4 Levels; however, one can use as many levels as deemed fit for the business/sector

Risk rating table example

Risk rating	Description	Risk Management Action
12-16	**Severe**	Needs immediate corrective action
8-12	**High**	Needs corrective action within 1 week
4-8	**Moderate**	Needs corrective action within 1 month
1-4	**Low**	Does not currently require corrective action

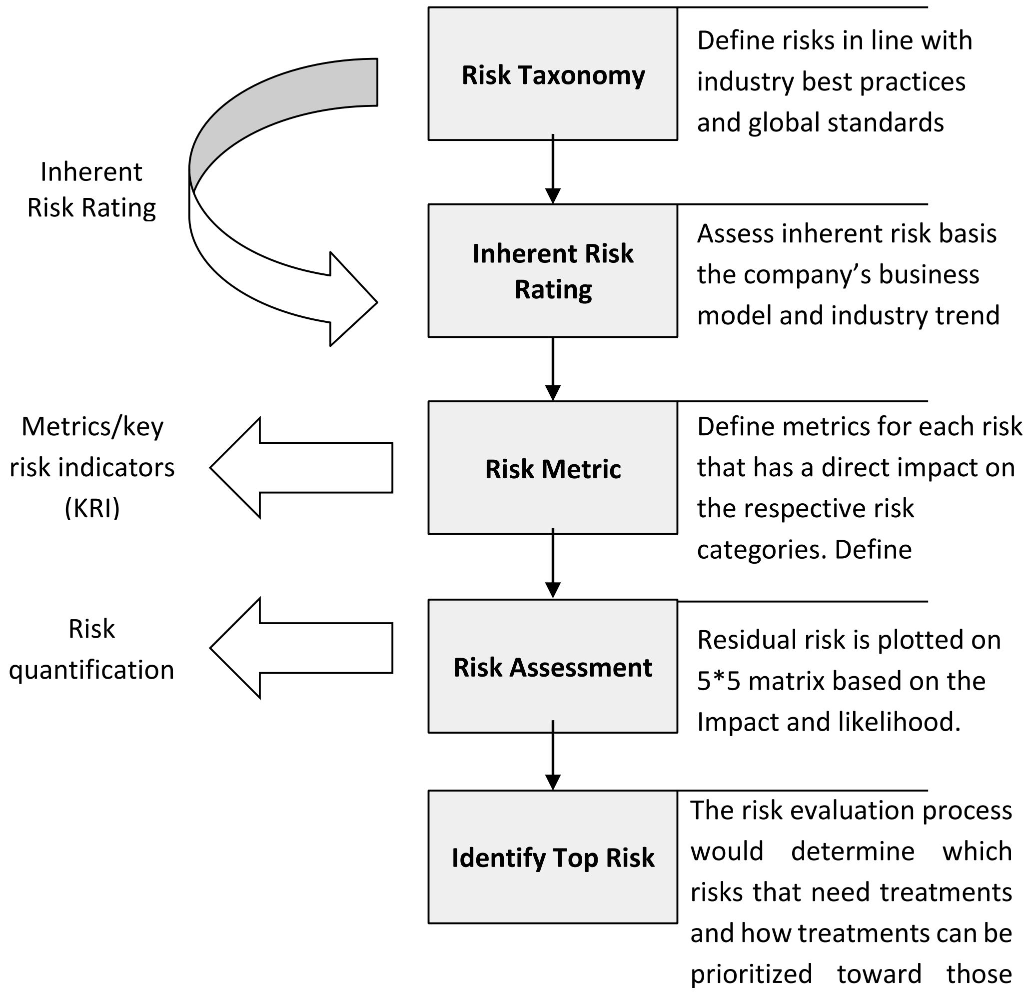
- Assess the likelihood of each identified risk occurrences. This involves analyzing historical data, expert opinions, statistical data, or other relevant information. Use qualitative or quantitative techniques, such as historical analysis, expert judgment, probability estimation, or data modeling, to determine the likelihood level.
- Evaluate the potential impact or consequences of each risk. Consider both the direct and indirect effects on various aspects, such as financial, operational, reputational, legal, safety, or environmental. Use qualitative or quantitative techniques, such as impact matrices, scenario analysis, cost estimation, or business impact analysis, to assess the impact level.

Scoring map 5*5 matrix based on impact and likelihood is

	Impact				
Likelihood	**1.Insignificant**	**2.Minor**	**3.Significant**	**4.Major**	**5.Severe**
1.Rare	**Low**	**Low**	**Low**	**Low**	**Low**
2.Unlikely	**Low**	**Low**	**Low**	**Low**	**Moderate**
3.Moderate	**Low**	**Low**	**Low**	**Moderate**	**High**
4.Likely	**Low**	**Low**	**Moderate**	**High**	**Severe**
5.Almost Certain	**Low**	**Moderate**	**High**	**Severe**	**Severe**

- Put the identified risks in order of importance based on a mix of their likelihood and impact. A risk matrix or other ranking techniques can be used to do this. Give each risk a risk priority or score to help concentrate resources and attention on the most important concerns.
- Create risk profiles for each one, taking into account all of their features. Included in this are a description of the risk, its origins, prospective effects, likelihood, impact, risk owner, and any pertinent information or proof that backs up the analysis. Effective decision-making and communication are aided by the risk profile.
- Few methodologies which can be used in Risk Assessment:
  - ➢ Conduct sensitivity analysis to understand the sensitivity of the risk; it explores the effect of changing individual risk variables on the overall outcome or results. It helps identify which variables have the most significant impact on the project or organization and assesses the robustness of the analysis to changes in those variables.
  - ➢ Cost-benefit analysis compares the costs of implementing risk mitigation measures against the expected benefits and helps in decision-making. It quantifies the costs associated with managing risks and assesses the potential value or savings that can be achieved by implementing risk reduction measures.
  - ➢ Event Tree Analysis (ETA) is a graphical technique used to analyze and evaluate the potential outcomes and consequences of specific initiating events or scenarios. It helps in understanding the sequences of events and their probabilities, which lead to different outcomes or states.

➢ Fault Tree Analysis (FTA) is a deductive technique used to analyze and assess the causes and effects of specific undesired events or failures. It involves representing the logical relationships between various events and failures using a graphical tree-like structure.



9. Risk Treatment

Risk Treatment is a crucial component of the risk management procedure. It involves implementing strategies and actions to manage identified risks effectively. The goal of risk treatment is to reduce the financial, likelihood, strategic, reputational and compliance impact or impact of risks to an acceptable level, while considering cost-effectiveness and the organization's risk appetite.

Key steps in Risk Treatment

Detailed review of risk treatment process is as follows:

- Before initiating the risk treatment process, review the results of the risk assessment. Revisit the identified risks, their likelihood and impact assessments, and overall risk prioritization. This step ensures that the treatment strategies are aligned with the identified risks.
- Identify and evaluate various risk treatment options for each identified risk. Common treatment options includes:

Acceptance	1.Acknowledge and accept the risk without taking any specific treatment actions. 2.This strategy is used for risks with low likelihood or impact.
Avoidance	1.Eliminate the risk by avoiding the activity or situation. 2.For e.g., changing project plans, avoiding certain business activities, or refraining from engaging in high-risk volume.
Mitigation	1.Implement measures to reduce the impact of risk. 2.For e.g., implementing controls, safeguards, redundancies, or process improvements.
Avoiding the risk by stopping	1.If the risk is deemed too significant or if the potential negative consequences outweigh the benefits, one possible approach is to consider avoiding the risk altogether by stopping the associated activity 2.Example: Ceasing a High-Risk Investment Strategy
Transfer	1.Transfer the risk to third party such as insurance, contracts, or outsourcing. 2.This strategy shifts the responsibility for managing the risk to another party.
Financing	1.Mitigating risk through financing the investment involves utilizing financial strategies and instruments to minimize potential losses and protect the investment. commodity price volatility.

Key steps in Risk Mitigations

Detailed review of risk treatment process is as follows:

Before initiating the risk treatment process, below steps are done:

- Review the results of the risk assessment,
- Revisiting the identified risks, their likelihood and impact assessments
- Overall risk prioritization: This step ensures that the treatment strategies are aligned with the identified risks
- Identification and evaluation of various risk treatment options for each identified risk
- Evaluation of available risk treatment options is done and selection of the most appropriate measures for each identified risk is taken.

Below are the factors taken into consideration

- Effectiveness of the treatment
- Cost-benefit analysis
- Resource availability
- Company's risk tolerance.

For each of the selected risks, treatment measures and development of a detailed risk treatment plan is framed with below:

- Specification of the actions
- Responsibilities
- Timelines
- Resources required to implement the treatment
- Clearly outlining the objectives
- Milestones
- Success criteria for monitoring
- Evaluating the effectiveness of the treatment

Risk treatment plans according to the established timelines and responsibilities are implemented and executed.

Maintenance of clear documentation of the implemented risk treatment measures, including the rationale behind their selection, implementation details, and ongoing monitoring results is ensured. Communication to the Risk Committee about the progress, effectiveness, and changes in risk treatment to relevant stakeholders, including senior management and risk owners is done every half year.

On-going monitoring, evaluation, and adaptation are essential to ensure that risk treatment remains relevant and aligned with the evolving risk landscape and organizational objectives.

10. Monitoring and Review

- **Risk Triggers:** We have defined Risk Triggers for each of the risks that are used to monitor the identified risks. These could include financial ratios, performance indicators, project milestones, or other relevant measures.

- **Establishing monitoring frequency:** As a prudent industry practice, risk monitoring is done twice a year or earlier as and when required.
- **Setting thresholds or benchmarks:** Defining the acceptable levels or thresholds for each risk indicator which help in identifying when risks are approaching or exceeding acceptable limits.
- **Collection and analyzing the data:** Continuous collection of relevant data related to the identified risk indicators. This may involve reviewing financial reports, project status updates, incident reports, or other sources of information.
- **Comparing actual performance to thresholds:** Regular comparison of collected data to the predetermined thresholds or benchmarks. Assessing whether the risk indicators are within acceptable limits or if they indicate an increased level of risk thereby indicating risk revision.
- **Identification of early warning signs:** Continuous monitoring of early warning signs that may indicate a potential increase in risk. These signs include trends, deviations from normal patterns, or specific triggers that have been identified as precursors to risk events.
- **Report findings:** Summarizing the monitoring results and communicating them to relevant stakeholders to provide a clear and concise overview of the current risk status, any emerging risks, and any necessary actions that need to be taken.
- **Taking corrective actions:** If the monitoring identifies risks exceeding the predetermined thresholds, initiation of appropriate mitigation measures or corrective actions are implemented. This involves revisiting risk mitigation strategies, reallocating resources, or implementing contingency plans.
- **Updating risk documentation:** Ensuring Risk register and other risk management documentation are up to date with the latest monitoring findings and documenting any changes in risk profiles, new risks identified, or updates to risk mitigation plans etc.

11. Risk Reporting

Risk reporting is a crucial component of the risk management procedure. It involves the systematic communication of information about identified risks, their potential impact, and the effectiveness of risk mitigation measures to relevant stakeholders. The purpose of risk reporting is to provide decision-makers with the necessary information to understand and manage risks effectively.

- The Risk Controller is responsible for reporting to the risk management committee and to the stakeholders.

The Risk Reporting consists of below activities:

- Action points and status against previous risk committee meeting
- Overall stakeholders interviewed
- Changes in Risk Register (Addition, Deletion, or any modification)
- Summary of High, Medium, and Low risks as per rating criteria and heat map
- Brief on Key High risks