Mahaana Wealth Limited

This Policy is effective immediately upon adoption and supersedes all previous risk management policies.

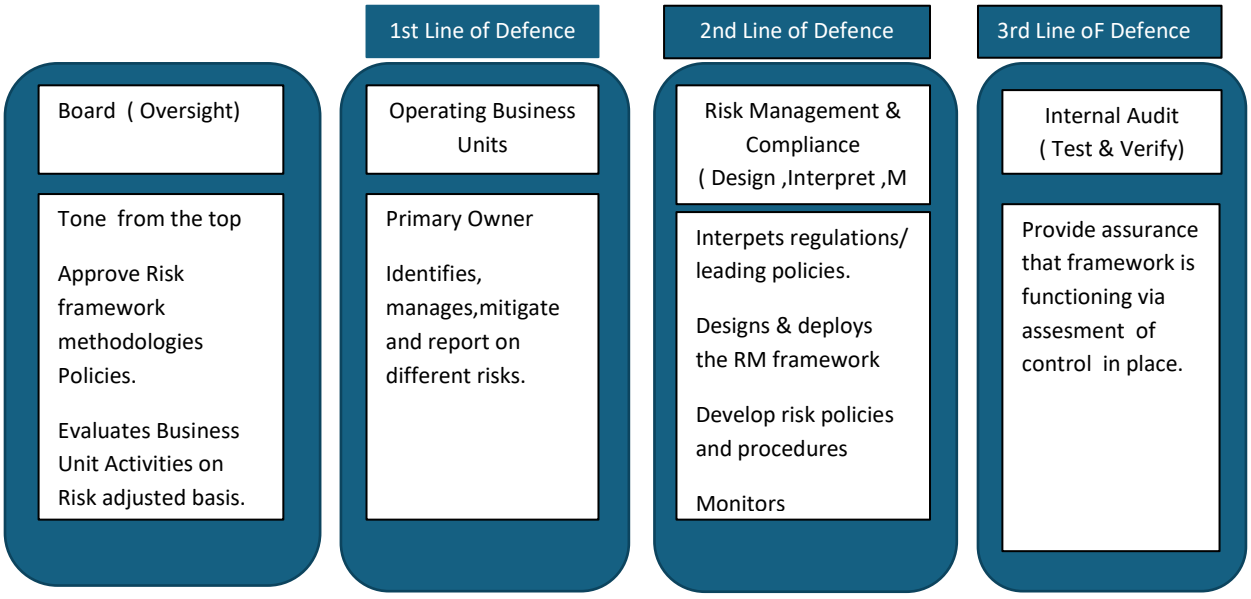
Prepared by Risk Management Department

1. PURPOSE

The Risk Management Policy Framework (the Policy framework) of the Mahaana Wealth Limited (the Company) has been developed to comply with the best practices of corporate governance and regulatory requirements concerning risk management. The Policy Framework provides principles for identifying, assessing, and monitoring risks faced by the company and the funds being managed by it. It specifies the key elements of the risk management process to maximize opportunities, minimize adversity, and achieve improved outcomes based on informed decision-making. The objective of this Policy is to ensure that prudent risk management practices have been adopted while managing collective investment scheme(s).

1.1 Risk Governance Structure:

The Risk Governance Structure in the Company is based on three (3) lines of defense framework. In this framework, the tone is set from the top by the Board and the BRMC. The Lines of defense are as follows:



1.2. Board of Directors (BOD)

Final authority and responsibility for all aspects of the conduct of activities that expose the company/scheme (s) to different types of risks rest with the BOD. The authority to conduct risk

monitoring and management activities from time to time shall be delegated to the Board Risk Management Committee (BRMC), the Investment Committee (IC), and other officials as per company policy. The BOD will ensure that management has established a framework for assessing risks and established methods for monitoring with the internal policies and regulatory requirements.

Further, the BOD will be responsible for:

- Understanding the risk profile of the collective investment scheme(s) and the tools used to manage all types of risks inherent to the scheme(s);
- Approving and reviewing risk management policies, strategies and management authority and responsibility;
- Ensuring that resources allocated for risk management are adequate given the size, nature, and volume of the business;
- Monitoring the risk profile dynamics periodically to continuously assess the risks faced by the company/scheme (s).

1.3 Board Risk Management Committee (BRMC)

BRMC is a board-level sub-committee with the primary responsibility of supervising the overall risk management function of the company/ collective investment scheme(s). It will decide the policy and strategy for the risk management containing various risk exposures to the Collective Investment Scheme(s):

Board Risk Management Committee	
Composition	• BOD Members • Member (Chief Executive Officer) • Other(s)
Chairman	As per the document of the Board of Directors
Secretary	Head of Risk
Minutes	To the concerned Functional Heads
Frequency of Meeting	At least once a Quarter
Reports	BRMC will be provided with all reports and information as may be necessary

The BRMC shall be responsible for:

- Ensuring that resource allocation for risk management is adequate given the size, nature, and volume of the business;
- Ensuring that the company/scheme has clear, comprehensive, and well documented policies and procedural guidelines relating to risk management.

- Reviewing policies and guidelines for identification, measurement, monitoring, and controlling of all major risk categories through interaction with the Head of Risk;
- Reviewing and approving market, liquidity and credit risks related limits;
- Reviewing the market, liquidity, credit, and operational risks exposures to the company/schemes.
- The BRMC will establish limits for the size of transactions that may be conducted by the Fund Manager(s) and the Investment Committee.
- Review the risk identification and management process developed by management to ensure consistency with the Company's strategy and business plan;
- Review the following with management, to obtain reasonable assurance that financial risk is being effectively managed and controlled:

a) Management of treasury funds of the company;
b) Nature and frequency of risk management reports
c) Management's assessment of significant financial risks facing the Company;

- Review limits assigned to different parties and financial institutions from time to time.

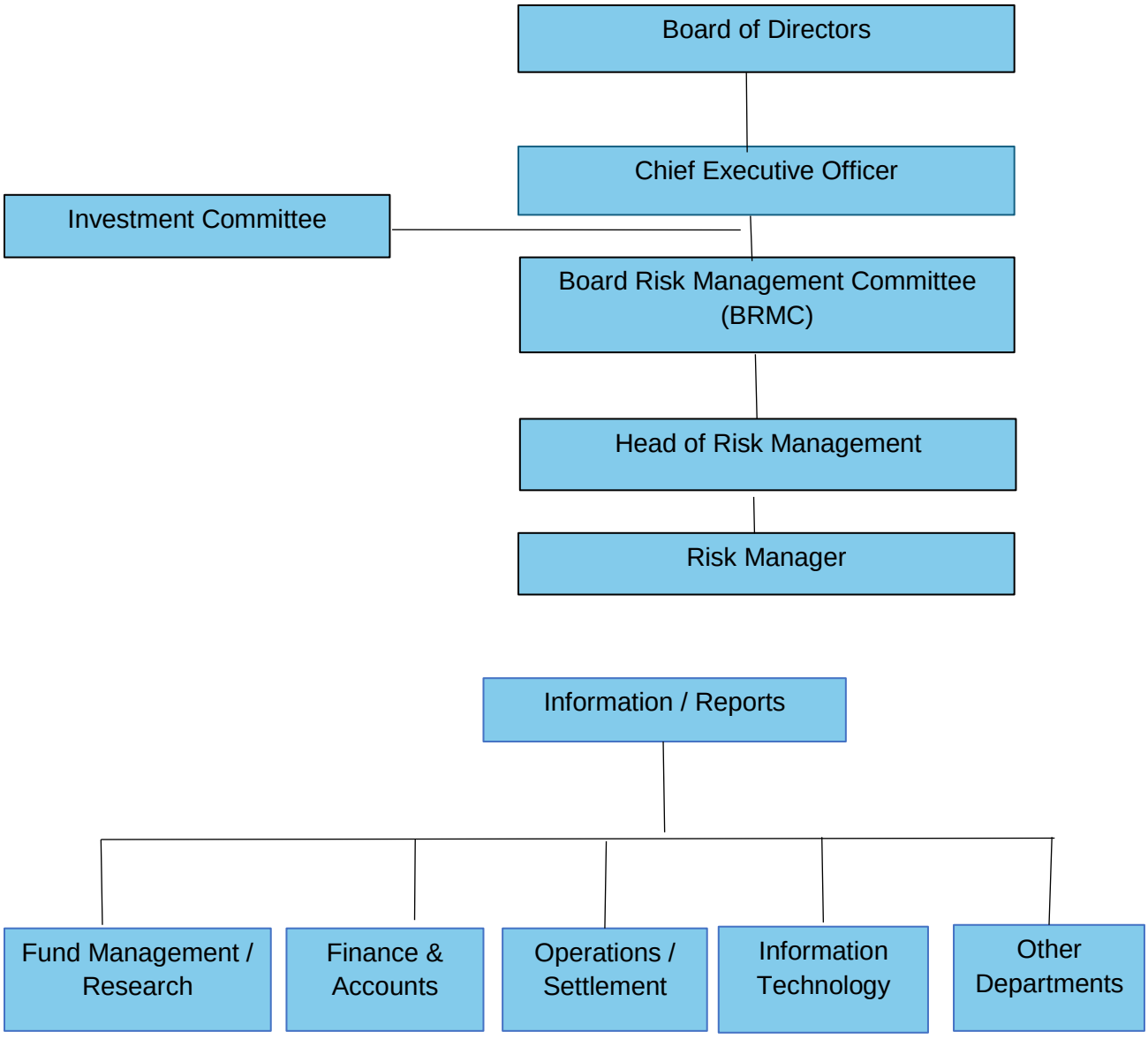
1.4 Investment Committee (IC)

The Investment Committee is entrusted with the overall responsibility to ensure the presence of an effective organizational structure that continuously monitor and manage the investment activities, market behavior, and economic trends:

Investment Committee	
Composition	• Chairman (Chief Executive Officer) • Member (Chief Investment Officer) • Member (Head of Equity) • Member (Head of Fixed Income) • Member (Fund Manager) • Member (Head of Research) • Member (Head of Risk Management) • Member (Digital Risk Unit) *
Chairman	Chief Executive Officer (CEO)
Secretary	Head of Research
Minutes	Secretary to the Committee
Frequency of Meeting	To be decided by the Chairman

*Digital Risk Unit- Specialized team responsible for cybersecurity, data privacy and IT infrastructure risks.

1.5 Risk Management Department



The Risk Management Department (RMD) is a specialized department that works closely with the risk-taking and supporting operations of the scheme(s). The function of RMD in the entire risk management framework is that of 'Monitoring and Reporting'.

The RMD will be staffed with people who have adequate knowledge, background, and skills to develop an understanding of the risk management function understand and identify business risks arising from

various activities of the scheme(s) and conduct analytical reviews using advanced analytical models and techniques.

1.6 Risk Management Standards

Risk Management Policy and Procedures will be based on lines of the following standards:

Risk Standard 1 - Acknowledgment of fiduciary responsibility

Fiduciary responsibilities shall be defined in writing and acknowledged in writing by the parties responsible. Fiduciary responsibility shall encompass the responsibilities of the BOD, Risk Committee including the CEO, Head of Risk Management, CIO, and the Risk Team members relating to risk management.

Risk Standard 2 - Approved written policies, definitions, guidelines, and investment documentation:

The Board of Directors (BOD) shall approve formal written policies. The procedures which reflect the overall risk management objectives of the company and funds under management as well as investment guidelines, management agreements, and all other contracts that govern Investments shall be approved by the senior management under delegated authority. All technical terms should be defined. All policies, definitions, guidelines, and investment documentation should be reviewed and updated as appropriate or more often if significant market events or changes in strategy occur. The risk policies shall apply both to internal and external managers (Third-party includes distributors & registrars from an operational perspective) and shall be consistent across similar asset classes and strategies.

Risk Standard 3 - Independent risk oversight, checks, and balances, written procedures and controls:

Oversight compliance with risk policies shall be independent of investment activity and conducted according to up-to-date, written policies and procedures. Front, middle, and back-office activities shall be separate, and sufficient checks and balances, and appropriate controls shall exist. The oversight function shall be conducted by the Board Risk Committee

Risk Standard 4 - Clearly defined organizational structure and key roles:

Organizational structure and reporting lines shall be defined clearly and distributed to all parties. It is important for the identification, measurement, and management of key risks. Key personnel and their roles in all fronts, middle and back-office areas shall be identified. Changes in key personnel should be communicated immediately to all relevant parties.

Risk Standard 5 - Adequate education, skill set, systems and resources, backup and disaster recovery plans:

The Board Risk Committee shall ensure that human resources with adequate education / skill set, systems, and resources are available to implement and administer the risk policy/procedures. There shall be a Code of Conduct /Ethics for the employees of the Company including policies to govern personal trades to counter the risk of insider trading, front running, and other misconduct.

Risk Standard 6 - Identification and understanding of key risks:

Risks shall be analyzed to determine relevancy in line with the Risk Profile of various investment portfolios. This entails understanding strategies and their vulnerabilities, as well as assumptions built into an instrument, system, process, model, or strategy. The concentration and interaction of various risk sources should also be analyzed. Key risks including key credit risks (i.e. credit watch list) should be reviewed periodically as well as when significant events occur

Risk Standard 7 - Setting risk limits:

Risk limits shall be set for the aggregate portfolio and all individual portfolios as well as for asset classes as the case may be. These may include limits on entities, asset classes, individual instruments, and specific types of risk e.g. Credit Risk, Market Risk, Liquidity Risk, etc. The methodology of defining risk limits in the form of Management Action Triggers (MATS) as the case shall be approved by the Board Risk Committee.

Risk Standard 8 - Routine reporting, exception reporting, and escalation procedures:

The Board Risk Committee shall specify reporting/escalation requirements of any risk limit breaches. This guideline also should define what constitutes required reporting or an exception to guidelines, who the exception should be reported to, what action must be taken for different levels of violation and what procedures must be followed for ongoing or increased violations. For routine reporting, the Risk Management Department shall decide the frequency and recipients.

Risk Standard 9 - Valuation procedures and reconciliations:

All readily priced instruments shall be valued daily. The pricing mechanism and methodologies must be known, understood, follow written policies, and be applied consistently by the Company Managers, trustee/custodians, and other subcontractors. Material discrepancies in valuations from different sources shall be reconciled following established procedures. The procedure for bid/offer adjustments and overrides to valuations shall be established in writing and monitored independently.

Risk Standard 10 - Risk measurement and risk/return attribution analysis:

The Risk Management Department shall regularly/periodically measure relevant risks and quantify the key drivers of risk and return. Risk-adjusted returns shall be measured by the Risk Management Department at the aggregate and individual portfolio level to gain a true measure of relative performance.

Risk Standard 11 - Stress testing of financial assets, Back-testing of strategies, and assessment of Model Risk:

Simulation or other stress tests shall be performed by the Risk Management Department to ascertain how the aggregate portfolio and individual securities would behave under various conditions. These

include changes in key risk factors, correlations, or other key assumptions and unusual events such as large market moves.

Risk Standard 12 - Due diligence, policy, and regulatory compliance and guideline monitoring:

The Internal Audit and/or Risk Management Department shall perform frequent, independent reviews of all departmental risk controls. Where controls fall short of the requirements, plans for future compliance or corrective action should be documented and communicated. Managers should ensure continuing compliance with the risk policies and guidelines. There will be zero tolerance for regulatory non-compliances.

Risk Standard 13 - Review process for new activities:

The Senior Management shall document the review process for permitting the use of new instruments, strategies, or asset classes. Policies for initiating new activities shall be consistent with the risk and return goals as well as the Manager's strategy and expertise.

Risk Standard 14- BCP and DSR

The Senior Management shall document the processes for BCP and Disaster Recovery Planning. It shall also establish and test backup procedures and disaster recovery/business continuity plan periodically.

2. TYPES OF RISK AND THEIR MANAGEMENT

Collective Investment Scheme(s) generate most of their revenues by accepting Market, Liquidity, Credit, Operational Risks and Cyber Security Risk. Effective management of these risks is the decisive factor in the profitability of the Company and its Funds. The Policy framework is organized concerning the following risk categories which are discussed below:

2.1 Market Risk

Market risk is the risk that the fair value or future cash flows of a financial instrument will fluctuate because of changes in market rates or prices such as interest rates, foreign exchange rates, equity prices, credit spreads, and/or commodity prices resulting in a loss to earnings and capital. Market risk comprises three types of risk:

1. Interest Rate Risk
2. Equity Price Risk
3. Currency Risk

Interest Rate Risk

Interest rate risk is the risk that the fair value or future cash flows of a financial instrument will fluctuate because of a change in market interest rates. Government securities (PIBs & T-Bills) and other money

markets & Fixed Income investments are subject to interest rate risk and these investments are here-in after referred to as interest-bearing securities

Interest Rate Risk Management

- The RM/BRMC/ IC shall be responsible for providing guidelines and/ or for making investment decisions in interest-bearing securities and setting exposure limits keeping in compliance with the regulations laid down by the SECP, Constitutive Documents, and other directives issued from time to time
- The BRMC/ IC shall review and approve exposure limits applicable to interest-bearing securities
- The RMD shall review and monitor the exposure limits and perform risk analysis using appropriate financial models to capture the sensitivity of the portfolio instrument to adverse movement in interest rates. Limit breaches/deviations shall be promptly reported to the senior management of the company.

Equity Price Risk

Equity price risk is the risk that the fair value or future cash flows of a financial instrument will fluctuate because of changes in market prices (Other than those arising from interest rate risk or currency risk), whether those changes are caused by factors specific to the individual financial instrument or its issuer, or factors affecting all similar financial instruments traded in the market.

Equity Price Risk Management

- The RMD/BRMC/ IC shall be responsible for making investment decisions in the Capital market and setting exposure limits assigned from time to time.
- The RMD shall be responsible for assigning portfolio, sector, and scrip wise limits to guard against Concentration Risk.
- The RMD/BRMC/ IC shall be responsible for providing guidelines and/ or for making investment/divestment decisions in the equity market and setting exposure limits keeping in compliance with the regulations laid down by the SECP, Constitutive Documents, and other directives issued from time to time.
- The RMD shall ensure alignment with limits set by RMD/BRMC/ IC. Limit breaches are promptly reported to Board Sub-Committees and/or Senior Management with proper reasoning (where required).
- The RMD shall perform risk analysis using appropriate financial model(s) for mitigating downside risk.

Currency Risk

Currency risk is the risk that the fair value or future cash flows of a financial instrument will fluctuate because of changes in foreign exchange rates. Investment in overseas markets and placements in foreign currency deposit accounts are subject to currency risk and are here-in- after referred to as foreign currency investments.

Currency Risk Management

- Investments abroad raising foreign currency risk shall be made after obtaining the prior approvals of the Securities and Exchange Commission of Pakistan (SECP) and the State Bank of Pakistan (SBP).
- The Board Risk Management Committee (BRMC)/ Investment Committee (IC) shall be responsible for making investment decisions and setting exposure limits for foreign currency investments keeping in view the regulations laid down by the SECP and other regulatory authorities and Constitutive Documents.
- All foreign currency investments shall be approved by higher authorities.
- The RMD shall monitor the net foreign currency exposure and the effect of exchange rate fluctuations by conducting risk analysis using the appropriate financial model. Limit breaches shall be promptly reported to the Board of Investment Committee (BRMC)/ Investment Committee (IC).

2.2 Liquidity Risk

Liquidity risk is the risk that an entity will encounter difficulty in meeting financial obligations associated with its financial liabilities due to the inability of liquidating an asset

Liquidity Risk Management

- The BRMC/ IC shall devise the liquidity management strategy to maintain sufficient liquidity for mitigating liquidity risk.
- The BRMC/ IC shall ensure that liquidity management strategy is adhered to continually.
- The BRMC/ IC shall monitor the maturities of assets and liabilities of the funds to identify any funding requirement in advance.
- The RMD shall devise the liquidity management model/ liquidity bucket that classifies the liquidity profile of the equity portfolio.
- The RMD shall perform a comprehensive risk analysis to prevent liquidity risk in case of extraordinary circumstances.

The liquidity buckets classify the category of liquid stocks of the portfolio and profiling of funds that indicate how many stocks in the portfolio are Highly Liquid, Liquid, Semi-Liquid and Illiquid and also indicates the percentage of readily available convertible assets to meet any potential redemption requests at any given time in future.

2.3 Credit Risk

Credit risk is the risk that one party to a financial instrument will cause a financial loss for the other party by failing to discharge an obligation. Credit risk can be categorized as “issuer credit risk” and “counterparty credit risk”.

i) Issuer Credit Risk: This is the risk of default or credit deterioration of an issuer of instruments that are held as long-term investments.

ii) Counterparty Credit Risk: Consists of both pre-settlement and settlement risks. Pre- settlement risks are the risk of loss due to the counterparty's failure to perform on a contract during the life of transaction whereas settlement risk is the risk of loss when a counterparty's mode of payment defaults.

Credit Risk Management

- The RMD shall develop a formalized and structured approach for the evaluation of the creditworthiness of the counterparty.
- The IC shall decide the eligibility criteria for the selection and approval of counterparties for credit transactions keeping in view the regulations laid down by the SECP in this respect and Constitutive Documents.
- If necessary, the RMD/BRMC/ IC shall establish guidelines for obtaining adequate collateral and follow appropriate credit evaluation criteria keeping in view the regulation laid down by SECP.
- The BRMC/ IC shall be responsible to ensure that the credit portfolio of the Fund exposed to credit risk is broadly diversified and transactions are entered into with diverse counterparties thereby mitigating credit risk.
- The RMD shall ensure compliance with the credit exposure limits, evaluation criteria laid down by BRMC/ IC, and regulations laid down by SECP.

<u>Credit Risk Scoring Model for Counterparty Risk Evaluation:</u>

Risk Management Department has developed a Counterparty Risk Scoring Model for all counterparties to assign internal credit risk limits. The Credit Risk Scorecard, as such, entails the weighted collection of both quantitative and qualitative factors equally. Quantitative scoring for financial institutions such as Banks/DFI is the composition of different financial ratios and the external credit rating.

a) Quantitative Analysis

This approach is being taken in calculating the quantitative scores based on the financial ratios of an entity while assigning an internal credit score. This method calculates the score from 2 dimensions, one is a peer comparison, and another is a historical comparison of the entity's financial ratios using the current number as a base.

b) Qualitative Analysis

The qualitative assessment includes different weighted factors, with the highest weight assigned to the external credit rating, assigned by PACRA and/or JCRVIS. RMD evaluates and makes a recommendation of the investment through Ratio Analysis of financial data, along with other pertinent information. It may evaluate potential investments and the credit worthiness of borrowers. The primary source of the data is extracted from the financial statements of the company under review.

c) Internal Credit limits

Internal Credit Limits for Collective Investment Scheme(s)

Internal credit limits are maintained based on the counterparty risk scoring model. We have assigned an internal rating to all counterparties from A to D where 'A' rating entity assigned maximum exposure (i.e.; 10% of net assets) and D rating entity assigned zero exposure.

Risk View	Internal Risk Rating	Internal Limit Assigned (% of Net Assets for Conventional)	Internal Limit Assigned (% of Net Assets for Islamic)
Positive	A	10.00%	15.00%
Neutral with a Positive Bias	B+	7.50%	11.25%
Neutral	B	5.00%	7.50%
Neutral with a Negative Bias	C	2.50%	3.75%
Negative	D	0.00%	0.00%

3. OPERATIONAL RISK MANAGEMENT

Definition

The operational risk is defined as follows:

a) "The risk of direct or indirect losses resulting from inadequate or failed internal processes, people, systems or external events"

Wherein direct loss and indirect loss is defined as:

b) "Direct loss has a negative impact on the entity's financial position. This impact can be observable on the entity's general ledger or can be traced to a series of events"

Indirect loss is defined as costs to identify, rework, and determine how to fix an existing problem.

c) Operational Risk Management Objectives and Strategy

The objective in implementing an entity-wide operational risk management framework is to:

- Protect the investor's long-term wealth;
- Provide employees with the best possible working environment to improve their morale and efficiency;
- Provide quality services, in the shape of facilitation, distribution and registrar services, to investors and potential investors to increase their confidence level in investing with us;

- Improve the financial strength and reputation in front of the stakeholders, especially the investors and regulatory authorities.

To manage the entity-wide operational risk, the company/scheme aims to:

- Implement an effective, consistent, and comprehensive risk management approach supported by sufficient resource allocation.
- Implement an independent risk management function with sufficient resources, authority, and expertise enhanced by an appropriate governance structure.
- Establish a board-level risk management committee to define standard framework components.
- Establish an accountability framework for risk management within the business units complemented by independent risk oversight of Internal Audit.
- Provide a consistent, high-level framework for monitoring and communicating risks supported by the ability to drill down into detailed risk management practices and information.
- Implement an effective, consistent, and comprehensive operational risk management framework supported by a set of principles, policies, and controls including code of conduct, authorization guidelines, business process standards, systems and process controls, and an approval process for the new product, investments, systems and procedures.

d) Operational Risk Categories

To manage entity-wide operational risk events, the company/scheme categorizes operational risk into the following four major categories.

i. People Risk

ii. Process Risk

iii. Systems Risk

iv. External Events Risk

3.1 People Risk Definition

People Risk can be defined as the risk of a loss intentionally or unintentionally caused by an employee - i.e. employee error, employee misdeed, etc. Risk Management Policy. The risk of loss related to the management and use of people, including inappropriate resource management, employee competency, and resource allocation and staffing tools. People risk management aims to minimize the losses that the company/scheme may incur due to inappropriate human resource management practices.

a) Sources of People Risk

People risk arises due to staffing inadequacy, unattractive remuneration structures, inadequate learning and development policies, unhealthy professional working relationships, unethical environment, etc.

b) People Risk Management

Effective personnel management is important to avoid the risk that arises from not having the right people with the right skills and attributes. The people's risk is managed by having appropriate policies for staffs' learning & development, performance measurement, remuneration, and retention. The company has a code of conduct and code of ethics, which are required to be read and signed by each employee. The Human Resource (HR) function will follow the board-approved employee service rules, policies, and procedures for staff hiring, termination, and resignations.

3.2 Process Risk Definition

Process risk is the risk of loss arising from inadequate or ineffective and inefficient business operations and processes.

a) Sources of Processes Risk

Process risk arises due to inadequate general controls and application controls, improper business & market practices and procedures, inappropriate/inadequate monitoring & reporting, and inadequate services.

b) Processes Risk Management

The company has put in place a strong internal control environment. A sound system of internal control is important to ensure the effectiveness and efficiency of operational processes, the reliability of financial reporting, and compliance with applicable laws and regulations.

3.3 Systems (Technology) Risk Definition

System Risk is defined as the risk of direct or indirect loss resulting from inadequate or failed system infrastructure of the company including all network, hardware, software, applications, communications, and their interfaces. The majority of the system-related risks are covered and will be mitigated via the implementation of an effective Information security policy.

a) Sources of Systems (Technology) Risk

System risk arises due to lack of information integrity, hardware failures, software failures, information security breaches, network failures, systems development, implementation risk, etc.

b) Systems (Technology) Risk Management

The company follows industry best practices to ensure information security, implementation of new systems, development of networks, etc. The company has policies and procedures for IT security, administration, and management covering key requirements such as Authentication and Identification, Access Control, Confidentiality, Encryption, Security Management, and Virus Control. This also includes

physical security i.e., protecting the IT system, and logical security in the form of user passwords and a firewall system. The company has measures to protect its records and programs against unauthorized changes.

3.4 External Event Risk Definition

This category of operational risk would include the following broad types of risks:

Disasters: The risk of loss due to damage to physical assets from natural or unnatural causes

Relationships: The risk of loss arising from the relationship or contact that the entity has with its investors, brokers, and service providers.

4. Cyber Security Risk

This category of Cyber Security Risk would include the following broad types of risks.

i. Multi- factor authentication (MFA) for all access point

- Multi-Factor Authentication is a security process that requires users to provide two or more verification factors to gain access to a system or application., to prevent unauthorized access and create extra layer of protection by requiring factors like OTP and biometric

ii. End to End encryption and secure APIs

- End-to-end encryption to protect data in transit, ensuring only intended recipients can access it. All APIs are secured with authentication, authorization, and encryption to prevent unauthorized access or data breaches.

iii. Annual Penetration testing and real time threat monitoring.

- Conducts annual penetration testing to identify and fix system vulnerabilities. We also maintain real-time threat monitoring to detect and respond to cyber threats instantly.

iv. Cyber incident response plan (CIRP) and teams

- Cyber Incident Response Plan (CIRP) quickly detects, responds to, and recovers from cyber incidents, to minimize impact from data breaches, ransomware, and system outages.

5. Anti- Money Laundering (AML) and know your customer (KYC) Risk

This category of risk relates to exposure to money laundering, terrorist financing, or other unlawful financial activities due to inadequate customer due diligence or monitoring controls.

- **Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD)**
  All customers are subject to risk-based due diligence measures. High-risk customers—such as politically exposed persons (PEPs), non-residents, or those from high-risk jurisdictions—are subject to Enhanced Due Diligence to verify identity, assess source of funds, and evaluate transaction behavior.

- **Sanctions screening and PEP identification**
  Customer data is continuously screened against domestic and international sanctions lists, watchlists, and PEP databases using automated tools to detect and prevent engagement with prohibited individuals or entities.
- **Ongoing monitoring and suspicious transaction reporting (STRs)**
  All customer transactions are monitored in real time for suspicious or unusual patterns. Identified anomalies are promptly reviewed and, where necessary, reported to the Financial Monitoring Unit (FMU) in the form of STRs or CTRs, as mandated by the Anti-Money Laundering Act, 2010.
- **Regulatory compliance and periodic reviews**
  The Compliance Department oversees the AML/KYC framework and ensures adherence to SECP Circulars, AML/CFT Regulations, and internal policies. Periodic risk assessments and internal audits validate the robustness of the controls.

6. Fraud Risk:

This category of risk pertains to intentional acts of deception or misrepresentation—either internal or external—that result in unauthorized benefit, financial loss, or reputational damage to Mahaana Wealth.

- **System Access Controls and Segregation of Duties**
  All critical operations — including account setup, transaction processing, and NAV calculations — are governed by system-enforced roles and approval hierarchies. No single employee has end-to-end access to client transactions or fund movement processes.
- **Biometric Verification and Two-Factor Authentication (2FA)**
  To prevent impersonation and account takeovers, all client access points are protected by biometric login and two-factor authentication (OTP-based), ensuring only verified users can initiate transactions.
- **Automated Fraud Detection and Exception Alerts**
  Mahaana's digital infrastructure includes real-time anomaly detection and transaction validation, flagging unauthorized or outlier activity. These alerts are investigated immediately by the Risk and Compliance teams.
- **Internal Audit and Digital Whistleblower Portal**
  An independent internal audit function periodically reviews system controls, transaction logs, and fraud management metrics. A secure, anonymous whistleblower portal is available for employees to report unethical behavior or suspected misconduct.
- **Incident Response and Corrective Actions**
  In the event of a confirmed fraud attempt or breach, Mahaana Wealth's incident response

protocol ensures immediate containment, investigation, stakeholder notification, and implementation of corrective actions, as per SECP requirements.

The Risk Management, Compliance, and Internal Audit departments collectively oversee the risk management process and are responsible for ongoing assessment and strengthening of internal controls.