UNIFI ASSET MANAGEMENT PVT LTD

Roles & Responsibilities of each CXOs and the CRO

The purpose of this document is to delineate the roles and responsibilities of key personnel involved in risk management activities, in alignment with the SEBI Risk Management Framework (RMF) circular issued on September 27, 2021.

This document outlines the specific roles and responsibilities for the following key positions:

- Chief Executive Officer (CEO)
- Chief Risk Officer (CRO)
- Chief Investment Officer (CIO)
- Fund Manager (FM)
- Chief Compliance Officer (CCO)
- Chief Operations Officer (COO)
- Chief Information Security Officer (CISO)

Role of Chief Executive Officer (CEO)

- The CEO is responsible for all risks at both the AMC and Scheme levels.
- The CEO must ensure that the outcomes of the risk management function are reported to him on a monthly basis.
- The CEO is tasked with defining the specific responsibilities of the CIO and CXOs regarding risk management.
- The CEO must define a risk appetite framework for schemes and the AMC.
- The CEO is responsible for defining appropriate risk metrics for respective CXOs, CIO, fund managers, etc.
- The CEO must ensure adherence to SEBI guidelines in respect of the Risk Management Framework (RMF) and relevant principles, including risk identification, risk management, risk reporting (both periodic and escalation of material incidents), and corrective actions taken, if any.
- The CEO is responsible for approving corrective actions on various findings and reporting to the board of AMC and trustees regarding the same, and escalating to the board of AMCs and trustees, if required, any major findings being reported.
- The CEO is responsible for the governance of Sales and Distribution Risk.
- The CEO must ensure adherence to SEBI guidelines in respect of RMF and relevant principles, including risk identification, risk management, risk reporting (both periodic and escalation of material incidents), and corrective actions taken.
- The CEO must define the Delegation of Power (DoP) and ensure adherence to the DoP framework of the Sales and Distribution network.
- The CEO must review the risk level for functional risk to ensure it is in accordance with the approved risk threshold and risk metric for the sales and distributor network.
- The CEO is responsible for formulating, reviewing, and periodically providing inputs to update the Risk and Control Self-Assessment (RCSA) for key risks and controls.
- The CEO must identify and implement corrective actions or recommend action plans for deviations in controls and present them to the Risk Management Committee.
- The CEO must monitor distribution channels and mis-selling incidents reported, such as the number of mis-selling incidents, negative comments in the inspection report relating to distribution, and analysis of the portfolio of investors, e.g., nature of investments vis-à-vis risk appetite of investors.
- The CEO must conduct performance reviews of distributors and review AMFI reports on enhanced due diligence performed for distributors, reporting any major deviations.

- The CEO must perform impact assessments of sales and promotion expenses, evaluating value added versus cost incurred.
- The CEO must implement monitoring tools over the usage of social media and take action for resolution in case of negative feedbacks, mentions, or comments.
- For material outsourcing activities, the CEO must perform adequate due diligence of outsourced vendors prior to onboarding and ensure periodic assessments are conducted in accordance with the outsourcing policy.
- The CEO is responsible for the governance of Talent Risk.
- The CEO must formulate, implement, and review Human Resources and remuneration policies and obtain approval from the Board of AMC.
- The CEO must define the Delegation of Power (DoP) and ensure adherence to the DoP framework for HR-related activities.
- The CEO must review the risk level for functional risk to ensure it is in accordance with the approved risk threshold and risk metric of the HR department.
- The CEO must formulate, review, and periodically provide inputs to update the RCSA for key risks and controls of the Human Resource Department.
- The CEO must identify and implement corrective actions or recommend action plans for deviations in controls and present them to the Board.
- The CEO must provide relevant information to the CRO regarding risk reports.
- For relevant functional risks, the CEO must identify, analyze, and report the following along with recommended action plans for early warning signals, emerging risks, major findings, near-miss and loss events, and fraud incidents.
- The CEO must ensure adequate backup and succession plans for key positions and key people are present at all times to ensure that the AMC is never deprived of the services of any Key Managerial Person (KMP).
- The CEO must ensure compliance with applicable laws with respect to staff, offices, etc.
- The CEO must ensure sales staff are NISM certified with the required qualifications prescribed by SEBI/AMFI.
- The CEO must escalate to the board of AMCs and trustees, if required, any major findings being reported.

Role of the Chief Risk Officer (CRO)

- The CRO is responsible for ensuring that there is an effective governance framework and reporting framework of risk management in line with regulatory requirements.

- The CRO must implement the risk management framework across the organization.
- The CRO is tasked with reviewing the specific responsibilities of management, including the CEO, CIO, CXOs, and Fund Managers.
- The CRO should establish a mechanism for risk reporting at least on a quarterly basis to the board of AMC, trustees, and RMCs, covering all risks including risk metrics, escalation of material risk-related incidents, and timely corrective actions taken, if any.
- The CRO is responsible for conducting an independent assessment of risk reporting to various committees and the CEO.
- The CRO must put in place a mechanism for reporting to the CEO, including outcomes for the risk management function on a monthly basis.
- The CRO ensures that risk reporting is independent from the CIO and verified by the risk team.
- The CRO must ensure there is a Delegation of Powers (DoP) approved by the Board of AMC for risk management, covering daily risk management, daily risk reporting, and corrective actions at the level of Fund Manager, CIO, and CEO.
- The CRO is responsible for informing the board of AMCs, trustees, and risk committees regarding any major findings or corrective actions required and updating them on the closure or status of various recommendations.
- The CRO must ensure adherence to the guidelines pertinent to SEBI in respect of the Risk Management Framework (RMF) and relevant principles, including risk identification, risk management, risk reporting (both periodic and escalation of material incidents), and corrective actions taken, if any.

Role of Chief Investment Officer (CIO)

- The CIO is responsible for the daily management of risk and necessary reporting relating to investment risk of all schemes, including market risk, liquidity risk, credit risk, and other scheme-specific risks such as compliance risk and fraud risk.
- The CIO must ensure adherence to the guidelines pertinent to SEBI in respect of the Risk Management Framework (RMF) and relevant principles, including risk identification, risk management, risk reporting (both periodic and escalation of material incidents), and corrective actions taken, if any.
- The CIO is tasked with defining the specific responsibilities of Fund Managers.
- The CIO must ensure adherence to the risk appetite framework and maintain the risk level for schemes.
- The CIO is responsible for calculating the overall risk by taking into account the weighted average of the risk-o-meter and the events of defaults. This includes

quantifying the overall risk by considering factors such as credit default, change in yield, change in NAV, external shocks, or unusual redemptions.

- The CIO must escalate any corrective actions taken to the CEO and the CRO.

Role of Fund Manager (FM)

- The FM is responsible for the daily management of investment risk for the managed schemes, including market risk, liquidity risk, credit risk, and other scheme-specific risks, and for appropriate risk reporting of any risk-related events to the CIO.
- The FM must ensure adherence to relevant SEBI guidelines in respect of the Risk Management Framework (RMF) and relevant principles, including risk identification, risk management, reporting, and corrective actions.
- The FM is tasked with ensuring adherence to the risk appetite framework to maintain the appropriate risk level for schemes.
- If there is a need to change the risk appetite of the scheme within the Product Risk Category (PRC) of that particular scheme, the FM must obtain approval from the CIO.
- The FM must take corrective action, if required, as per the approved Delegation of Powers (DoP) and escalate any major risk-related events to the CIO.

Role of Chief Compliance Officer (CCO)

- The CCO is responsible for the governance of Compliance Risk within the organization.
- The CCO must ensure adherence to SEBI guidelines in respect of the Risk Management Framework (RMF) and relevant principles, including risk identification, risk management, risk reporting (both periodic and escalation of material incidents), and corrective actions taken.
- The CCO is tasked with ensuring adherence to applicable SEBI regulations and circulars issued from time to time.
- The CCO must formulate, implement, and review policies in accordance with the SEBI Risk Management Framework, as approved by the Board of AMC and Trustees.
- The CCO is responsible for defining the Delegation of Power (DoP) and ensuring adherence to the DoP framework.
- The CCO must review the risk level for functional risk to ensure it is in accordance with the approved risk threshold and risk metric.
- The CCO is responsible for formulating, reviewing, and periodically providing inputs to update the Risk and Control Self-Assessment (RCSA) for key compliance risks and controls, and for performing and reporting the outcomes of periodic testing of the RCSA to the CRO.
- The CCO must identify and implement corrective actions or recommend action plans for deviations in controls and present them to the CRO and CEO.

- The CCO must provide relevant information to the CRO regarding risk reports.
- The CCO is responsible for identifying, analyzing, and reporting early warning signals, emerging risks, major findings, near-miss and loss events, and fraud incidents to the CRO and CEO along with recommended action plans.
- The CCO must ensure the identification and communication of regulatory updates to the respective functions and CXOs and monitor their implementation.
- The CCO must ensure timely and accurate filing of regulatory reports, returns, and filings to the Regulator, Board of AMC, and Trustees as prescribed by SEBI Mutual Funds Regulation.
- The CCO is responsible for monitoring scheme-related disclosures, including the disclosure of credit quality of investments made, mainly debt based on the credit rating, counterparty, investment, and other risks associated with the scheme to the investors.
- The CCO must ensure the scheme's risk profile (including PRC) is stated in all communications with investors, including in the SID and marketing materials, and incorporate any other elements of risk appetite as may be stipulated by AMCs and Trustees in the SID.
- The CCO must implement processes for the prevention or detection of possible insider trading at the personnel or portfolio levels.
- The CCO is responsible for implementing processes for performing compliance checks of AMC's marketing materials (collateral, brochures, etc.), website uploads, digital advertising, and performance advertising before their usage.
- The CCO must ensure that the roles and responsibilities of CXOs are disclosed on the AMC website.
- The CCO is responsible for reviewing the complaint resolution process.
- The CCO must maintain all required SEBI-related licenses, registrations, approvals, and permissions.
- The CCO must ensure there is a Chinese wall between different businesses carried out by the Asset Management Company (such as PMS, AIF, Overseas Investments, Advisory, Mutual Funds, etc.).

Role of Chief Operations Officer(COO)

- The COO is responsible for the governance of Operational Risks, Financial Reporting Risk, and Legal & Tax Risk.
- The COO must ensure adherence to SEBI guidelines in respect of the Risk Management Framework (RMF) and relevant principles, including risk identification, risk management, risk reporting (both periodic and escalation of material incidents), and corrective actions taken.

- The COO is tasked with ensuring adherence to applicable SEBI regulations and circulars issued from time to time.
- The COO must formulate, implement, and review policies in accordance with the SEBI Risk Management Framework, as approved by the Board of AMC and Trustees.
- The COO is responsible for defining the Delegation of Power (DoP) matrix and ensuring adherence to the DoP framework.
- The COO must review the risk level for functional risk to ensure it is in accordance with the approved risk threshold and risk metric.
- The COO is responsible for formulating, reviewing, and periodically providing inputs to update the Risk and Control Self-Assessment (RCSA) for key risks and controls, and for performing and reporting the outcomes of periodic testing of the RCSA to the CRO.
- The COO must identify and implement corrective actions or recommend action plans for deviations in controls and present them to the CRO and CEO.
- The COO must provide relevant information to the CRO regarding risk reports.
- For relevant functional risks, the COO must identify, analyze, and report early warning signals, emerging risks, major findings, near-miss and loss events, and fraud incidents to the CRO and CEO along with recommended action plans.
- The COO must ensure the implementation of an integrated investment management system across the front office, mid office, and back office.
- The COO must adhere to the Investment Valuation Policy.
- The COO is responsible for establishing detailed accounting policies and procedures for mutual fund accounting.
- The COO must ensure the documentation and testing of internal controls over financial reporting for mutual fund schemes.
- For material outsourcing activities, the COO must perform adequate due diligence of outsourced vendors prior to onboarding and ensure periodic assessments are conducted in accordance with the outsourcing policy.

Role of Chief Information Security Officer (CISO)

- The CISO is responsible for the governance of Technology, Information Security, and Cyber Risk.
- The CISO must ensure adherence to SEBI guidelines in respect of the Risk Management Framework (RMF) and relevant principles, including risk identification, risk management, risk reporting (both periodic and escalation of material incidents), and corrective actions taken.

- The CISO must formulate, review, and periodically provide inputs to update the Risk and Control Self-Assessment (RCSA) for key risks and controls, and perform and report the outcomes of periodic testing of the RCSA to the CRO.
- The CISO must identify and implement corrective actions or recommend action plans for deviations in controls and present them to the CRO and CEO.
- The CISO must provide relevant information to the CRO regarding risk reports.
- For relevant functional risks, the CISO must identify, analyze, and report early warning signals, emerging risks, major findings, near-miss and loss events, and fraud incidents to the CRO and CEO along with recommended action plans.
- The CISO must ensure implementation of systems and processes as elaborated in Cyber security circulars released by SEBI.
- The CISO is responsible for conducting Business Continuity Plan (BCP) testing and Disaster Recovery (DR) drills.
- The CISO is responsible for framing & implementing IT policies in accordance with the circulars released by SEBI / AMFI from time to time.
- The CISO is responsible for reviewing audit observations and taking corrective actions in the Vulnerability Assessment and Penetration Testing (VAPT) audit and cybersecurity and systems audit.
- The CISO must ensure adherence to guidance provided by the Technology Committee of the Board.
- For material outsourcing activities, the CISO must perform adequate due diligence of outsourced vendors prior to onboarding and ensure periodic assessments are conducted in accordance with the outsourcing policy.