

## **Roles and Responsibilities pertaining to Risk Management**

### **MD & Chief Executive Officer**

- a. Responsible for all risks at both AMC and Scheme level
- b. Review the outcomes of Risk Management Function on a monthly basis.
- c. Approve roles and responsibility including KRA of Chief Investment Officer ("CIO") Chief Risk Officer (CRO) and other CXOs regarding risk management
- d. Define risk appetite framework for schemes and AMC
- e. Define risk metric for respective CXOs, CIO and Fund managers
- f. Ensure adherence to the guidelines pertinent to SEBI in respect of RMF and relevant principles thereunder including risk identification, risk management, risk reporting (both periodic and escalation of material incident) and corrective actions taken, if any.
- g. Approve, report and escalate corrective actions on major findings to the Board of AMC and Trustee.
- h. Establishing an organization-wide risk-conscious culture.

### **Chief Risk Officer (CRO)**

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

The roles of the CRO are as under:

- a. Implementation of Risk management framework across the organization.
- b. Review specific responsibility of management, including CEO, CIO, CXOs, and Fund Managers pertaining to risk management.
- c. Put in place 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, timely and corrective actions taken, if any.
- d. Independent assessment of reporting of risk to various committees and CEO, etc.
- e. Put in place mechanism for reporting to CEO - Including outcomes for risk management function on monthly basis.
- f. The reporting of risk as above is independent from the CIO and verified by the risk team.
- g. There is a DoP approved by the Board of AMC for risk management by CRO covering the following:
  - i. Daily risk management
  - ii. Daily risk reporting
  - iii. Corrective actions at the level of Fund manager, CIO and CEO.
- h. To inform the Board of AMCs, Trustee and Risk Committees regarding any major findings or corrective actions required and also update on closure or the status of various recommendations.
- i. The role in the Investment Committees of the MF, PMS, AIF and the AMC as well as the Valuation Committees is to provide a risk and governance perspective with respect to internal standards, processes and investment/valuation policies.
- j. The role in the Product Committee is to provide a perspective on the market risk as well as operational risk of the proposed new product/proposed change in product and the proposed internal limits/processes for the same.

- k. For Information Security, to direct the development of policies, procedures and standards for assessing information security risks, determining the appropriate security measures and for performing security audits.
- l. Establishing an organization-wide risk-conscious culture.
- m. Keeping the Board of AMC and Trustees informed on new or emerging risks.

#### **Chief Investment Officer**

- a. Responsible for daily management of risk and necessary reporting relating to Investment risk of all scheme(s) such as market Risk, liquidity Risk, credit risk, governance risk, etc. and other scheme specific risks (Compliance Risk, Fraud Risk, etc.)
- b. Ensure adherence to the guidelines pertinent to SEBI in respect of RMF and relevant principles thereunder including risk identification, risk management, risk reporting (both periodic and escalation of material incident) and corrective actions taken, if any.
- c. Define specific responsibility of Fund Managers
- d. Ensure adherence to risk appetite framework as applicable to the schemes and maintain risk level for schemes
- e. Calculate the overall risk by taking in to account the weighted average of (i) the risk-o-meter and (ii) the events of defaults. Both (i) and (ii) are to be calculated in terms of a number taking into account the risk-o-meter and events of defaults or early mortality of investments which may inter alia include credit default, change in yield, change in NAV, external shock or unusual redemptions, etc. to quantify the overall risk.
- f. Monitoring and Reporting of instances of deviation to appropriate forums along with rationale and corrective actions taken.
- g. Escalate the corrective actions taken, if any, to the CEO and the CRO

#### **DMD & Joint CEO (Chief Business Officer (CBO))**

- a. Responsible for the governance of risks within the function including operational risk, Business risk, Sales and distribution risks, Reputation risk, etc.
- b. Define specific responsibility regarding risk management of reportees.
- c. Ensure functioning in line with internally approved risk policies/thresholds, as applicable.
- d. Ensure adherence with the DoP framework.
- e. Take immediate action for non-compliance or major findings/incidents post approval from CEO as per DoP and shall ensure reporting to CRO
- f. Formulate, review and periodically provide inputs to update the RCSA for key risks and controls
- g. Adherence to the guidelines pertinent to SEBI in respect of RMF and relevant principles thereunder including risk identification, risk management, risk reporting (both periodic and escalation of material incident) and corrective actions taken
- h. Ensure risk reporting/ incident escalation as per defined process

#### **Chief Compliance Officer (CCO)**

- a. Responsible for the governance of risks within the function including operational risk, Compliance risk, Legal risk, etc.
- b. Define specific responsibility regarding risk management of reportees.
- c. Ensure functioning in line with internally approved risk policies/thresholds, as applicable

- d. Ensure adherence with the DoP framework
- e. Formulate, review and periodically provide inputs to update the RCSA for key risks and controls
- f. Take immediate action for non-compliance or major findings post approval from CEO as per DoP and shall report to CRO
- g. Adherence to the guidelines pertinent to SEBI in respect of RMF and relevant principles thereunder including risk identification, risk management, risk reporting (both periodic and escalation of material incident) and corrective actions taken
- h. Ensure risk reporting/ incident escalation as per defined process

#### **Chief Operating Officer (COO)**

- a. Responsible for the governance of risks within the function including Operational risks, Financial Risk, Outsourcing Risk, Reputation Risk, Legal & Tax Risk, etc.
- b. Define specific responsibility regarding risk management of reportees.
- c. Ensure functioning in line with internally approved risk policies/thresholds, as applicable
- d. Ensure adherence with the DoP framework
- e. Formulate, review and periodically provide inputs to update the RCSA for key risks and controls
- f. Take immediate action for non-compliance or major findings post approval from CEO as per DoP and shall report to CRO
- g. Adherence to the guidelines pertinent to SEBI in respect of RMF and relevant principles thereunder including risk identification, risk management, risk reporting (both periodic and escalation of material incident) and corrective actions taken
- h. Ensure risk reporting/ incident escalation as per defined process

#### **Chief Digital and Technology Officer**

- a. Responsible for the governance of risks within the function including operational risk, Technology and Information Security risk, reputation risk. etc.
- b. Define specific responsibility regarding risk management of reportees.
- c. Ensure functioning in line with internally approved risk policies/thresholds, as applicable
- d. Ensure adherence with the DoP framework
- e. Formulate, review and periodically provide inputs to update the RCSA for key risks and controls
- f. Take immediate action for non-compliance or major findings post approval from CEO as per DoP and shall report to CRO
- g. Adherence to the guidelines pertinent to SEBI in respect of RMF and relevant principles thereunder including risk identification, risk management, risk reporting (both periodic and escalation of material incident) and corrective actions taken
- h. Ensure risk reporting/ incident escalation as per defined process

#### **Chief Information Security Officer**

- a. Responsible for the governance of Information Security risk
- b. Define specific responsibility regarding risk management of reportees.
- c. Ensure functioning in line with internally approved risk policies/thresholds, as applicable

- d. Ensure adherence with the DoP framework
- e. Formulate, review and periodically provide inputs to update the RCSA for key risks and controls
- g. Take immediate action for non-compliance or major findings post approval from CRO and CEO as per DoP
- i. Adherence to the guidelines pertinent to SEBI in respect of RMF and relevant principles thereunder including risk identification, risk management, risk reporting (both periodic and escalation of material incident) and corrective actions taken.
- j. Ensure risk reporting/ incident escalation as per defined process.

**Chief Human Resource Officer (CHRO)**

- a. Responsible for the governance of risks within the function including operational risk, Talent risk, reputation risk, etc.
- b. Define specific responsibility regarding risk management of reportees.
- b. Ensure functioning in line with internally approved risk policies/thresholds, as applicable
- c. Ensure adherence with the DoP framework
- d. Formulate, review and periodically provide inputs to update the RCSA for key risks and controls
- f. Take immediate action for non-compliance or major findings post approval from CEO as per DoP and shall report to CRO
- g. Adherence to the guidelines pertinent to SEBI in respect of RMF and relevant principles thereunder including risk identification, risk management, risk reporting (both periodic and escalation of material incident) and corrective actions taken
- h. Ensure risk reporting/ incident escalation as per defined process.
- i. Establishing human resource practices pertaining to hiring, orientation and training in order to send messages to employees regarding the organization's expected standards on integrity, ethical behavior, competence and risk management