Risk Management Policy

Version 6

This document will be reviewed once annually and whenever there is a significant change to the business, to ensure continual alignment with the current needs of the Organization

Document owner	Jeyaraman K
Date of current issue	18-April-2023
Version	6

Background

The Company recognizes that risk is inherent to any business activity and that managing risk effectively is critical to the immediate and future success of the Company. Further, extant regulations mandates that risk management policy of the Company provides a framework to identify, assess and manage potential risks and opportunities impacting the business objectives of the Company.

SEBI's circular ref. SEBI/HO/MIRSD/DoP/CIR/P/2018/ 119 dated August 10, 2018, on enhanced monitoring of Qualified Registrars to an Issue and Share Transfer Agents (referred as QRTAs hereinafter, which is defined as RTAs servicing more than 2 crore folios) also recommend the following:

- ✓ QRTAs may be required to comply with enhanced monitoring requirements, through adoption and implementation of internal policy framework, and periodic reporting on key risk areas, data security measures, business continuity, governance structures, measures for enhanced investor services, service standards, grievance redressal, insurance against risks, etc.
- ✓ QRTAs were also advised to formulate and implement a comprehensive policy framework, approved by the Board of Directors ("BoD") of the QRTAs, which should include Risk Management Policy.

Purpose

The Risk Policy lays down a framework for identifying and determining the aggregate risk in the client operations, evaluating it considering the risk appetite of the business, and to place risk control measures in place to alert managers and to control risks within acceptable parameters. The framework envisages continuous improvement in risk management and ensuring adequate risk mitigation measures, to avoid any liability on the Organization, as a whole.

In line with the Company's objective towards increasing stakeholder value, a risk management policy has been framed, which attempts to identify the key events / risks impacting the business objectives of the Company and attempts to develop risk policies and strategies to ensure timely evaluation, reporting and monitoring of key business risks.

Risk Management Policy Statement

CAMS recognizes that it is exposed to number of uncertainties, which is inherent for the financial sector that it operates in. The volatility of the sector affects the financial and non-financial results of the business. CAMS has devised this Risk Management Policy to increase confidence in the achievement of organization's objectives and to remain a competitive and sustainable organization and enhance its operational effectiveness.

The risk management policy statement of CAMS is stated as follows:

- To formulate a detailed risk management policy which shall include:
    - A framework for identification of internal and external risks specifically faced by the entity, including financial, operational, sectoral, sustainability (particularly, ESG related risks), information & cyber security risks or any other risk as may be determined by the Risk Management Committee.
    - Measures for risk mitigation including systems and processes for internal control of identified risks.
    - Business continuity plan.

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

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

- To periodically review the risk management policy, at least once in a year, including by considering the changing industry dynamics and evolving complexity.

- To keep the board of directors informed about the nature and content of its discussions, recommendations, and actions to be taken.

- The appointment, removal, and terms of remuneration of the Chief Risk Officer (if any) shall be subject to review by the Risk Management Committee. The Risk Management Committee shall coordinate its activities with other committees, in instances where there is overlap with activities of such committees, as per the framework laid down by the Board of Directors.

- To establish an integrated Risk Management Framework for identifying, assessing, mitigating, monitoring, evaluating, and reporting of all risks.

- To provide clear and strong basis for informed decision making at all levels of the organization.

- To continually strive towards strengthening the Risk Management System through continuous learning and improvement and to achieve the objectives of this policy through proper implementation and monitoring.

- To ensure that new emerging risks are identified and managed effectively.

- To put in place systems for effective implementation for achievement of policy objectives through systematic monitoring and effecting course corrections from time to time.

Objective

- To manage risks with an institutionalized framework and consistently achieving desired outcomes

- To protect and enhance enterprise Value and enhance Corporate Governance

- To implement a process to identify potential / emerging risks

- To implement appropriate risk management initiatives, controls, incident monitoring, reviews, and continuous improvement initiatives

- Minimize undesirable outcomes arising out of potential risks

- To align and integrate views of risk across the enterprise

Roles & Responsibilities of stakeholders

- **Employees**: Every employee of the CAMS plays vital role in the risk management vigilance including identification of risks, reporting, and implementing suitable control measures thereof as mandated to them and protect overall company's financial and reputational impact.

- **Risk Management team** has a significant role in the development, maintenance, and implementation of Risk Management Policies.

- **Senior Management team's** commitment is a prerequisite to successful implementation of this policy, and they are responsible for managing risks associated with each of the processes and ensure adherence to the risk mitigation measures communicated from time to time. CAMS have nominated the Chief Risk Officer as the responsible person, for championing the maintenance and implementation of this policy.

- **Internal Risk Management Committee** will have overall oversight, determine, and communicate policy, objectives, procedures & guidelines, direct and monitor implementation, practice, and performance throughout CAMS.

- **Board level Risk Management Committee** shall review and approve Risk Management policy from time to time. This committee will assist the Board of Directors in fulfilling its corporate governance and overseeing responsibilities in relation to an entity's financial reporting, internal control system, and risk management system including the risk parameters. This Committee shall also review the internal audit reports, compliance to SEBI Regulations, circulars.

- **Board of Directors** should get apprised of the Risk Management Committee activities and would monitor the highly critical risk events / incidents having an impact on investor protection, large financial liability and data security breaches that can affect investor data, Frauds, etc.

Core Principles

To achieve the objectives, CAMS shall adhere to the following core principles:

1. **Risk Culture**

Operational risk at CAMS stems from our contractual obligations to hold and process client financial data. Therefore, our Risk Culture is extremely conservative. We will make every effort to mitigate operational risk and shall evaluate every change through a risk spectrum. Clients shall be made aware of operations risk, as and when we perceive the same.

2. **Risk Appetite**

We recognize that in some instances, our clients outsource activities to us, to remove an element of risk from them and pass them on to us, where they expect a greater level of risk management. Notwithstanding the conservative Risk Culture, the nature of our business is such that errors do occur, and risk cannot be eliminated. Given the impossibility or commercial infeasibility of eliminating Risk, we need to recognize our Risk Appetite. This must be solidified by means of internal discussions and discussions with clients. Various clients support our Risk Policy to varying degrees, and therefore our Risk Appetite to an extent is dependent on the client's Risk Appetite.

3. Risk Identification and Evaluation

Operations Risks are arising out of internal and external events. Internal events include IT and Systems risk, processing and other human errors, people risk, employee negligence / fraud etc. External Risk events includes Natural/Man-made disasters, market movements, client actions/business rules resulting in risk exposure, third-party fraud(s), etc. There is a need to have an ongoing process to identify and centrally record all operational risks.

Having identified a risk, evaluate its impact by assessing the consequences, if the risk materializes, resultant impact and assigning a probability for the risk to materialize. This risk evaluation, in conjunction with our risk appetite, will form the basis for the risk control measures.

4. Risk Exposure Monitoring

Aggregate Risk Exposure must be monitored to the best of our ability. While ideally this would be measured in tangible terms, at the very least, we should be able to measure individual business units using Risk Indicators in relative terms on a scale between comfortable to unacceptably high. Aggregate Risk Exposure should be a mandatory part of client reviews so that clients participate in the process of risk mitigation.

5. Risk Control

Risk cannot be eliminated but can be controlled. Risk Control measures are not to be imposed as a layer; they are to be built into the very operating procedures. To ensure that these operating procedures have the requisite degree of risk control built in, there are audit and other measurement tools.

Insurance Cover must be used as a tool to cover financial losses out of the Aggregate Risk Exposure. Accurate identification of Aggregate Risk Exposure will result in appropriate amount and type of insurance coverage. Insurance cover should be taken with large unrelated insurers to mitigate counterparty risk.

Since all Insurance Covers have “excess” or “self-insurance” element, the operating budget must provide for the value of expected financial losses arising out of the self-insured component of Aggregate Risk Exposure.

6. Transparency and Compliance

The risk management activities along with the most significant risks shall be reported and the material failures in mitigation measures shall be escalated through reporting line to the relevant levels of organization structure.

7. Incident Escalation and Data Collection

Every incident of a materialized nature or a “near miss,” resulting in financial claims or breach of compliance or investor escalation impacting the reputation either of AMC or CAMS, must be recorded, and reported to the Risk Management functions by the relevant stakeholders. These incident reports should describe the brief about the incident, including potential claims, if any and cover the controls implemented to prevent recurrence of similar incidents. These incidents will be reviewed by the Risk committee including recording of decisions and preventive actions. The lessons learnt through the reports could be in the form of recognizing a new risk type itself or, in the form of recognizing that the likelihood of a risk occurring had materially changed due to environmental factors etc. Over Time, escalating and cataloguing will provide Risk Managers with a database of events that they can then use to fine tune their Risk Control measures.

Document Control

Version	Date	Changed by	Reviewed by	Remarks on Change
1	1st April 2018	S V Karthick Babu	Jeyaraman K	-
2	6th Feb 2019	Reeta. X	Jeyaraman K.	Roles & Responsibilities
3	7th July 2020	S V Karthick Babu	Jeyaraman K	Reviewed and minor modifications done.
4	12th May 2021	Vidya Krishnaswamy	Jeyaraman K	Policy got amended in line with recent change in LODR
5	15th June ‘22	Ajay Rajan	Jeyaraman K	Annual review with minor modifications
6	18th April ‘23	Ajay Rajan	Jeyaraman K	Reviewed and No Changes

Owner: Risk Management team
Month of Review: April 2023

Annexure

Terms and Definition

Risk:
Risk is often described as an event, a change in circumstances or a consequence that may occur, and whose occurrence, if it does take place, has a harmful or negative impact on the achievement of the organization's business objectives. Thus, risk is the effect of uncertainty on objectives.

Risk Management:
Risk Management is the coordinated activities to direct and control an organization about risk. It is the process whereby organizations methodically address the risks attached to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities.

Risk Management Policy:
Risk Management Policy is a statement of the overall intentions and direction of an organization related to Risk Management.

Risk Management Framework:
Risk Management Framework is a set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving Risk Management throughout the organization.

Risk Management Plan:
Risk Management Plan is a scheme or an operation plan within the Risk Management Framework specifying the approach, management components and resources to be engaged for the management of risk.

Risk Strategy:
The Risk Strategy of an organization defines its readiness towards dealing with various risks associated with the business. It describes the organization's risk appetite or tolerance levels and decision to transfer, reduce or retain the risks associated with the business.

Risk Owner:
Risk Owner is a person or entity with the accountability and authority to manage risk.

Risk Assessment:
Risk Assessment is defined as the overall process of risk identification, risk analysis and risk evaluation.

Risk Estimation:
Risk Estimation is the process of carrying out quantitative, semi-quantitative or qualitative assessment of risk in terms of the probability of occurrence and the possible consequence.

Risk Identification:
Risk Identification is a process of finding, recognizing and describing risks.

Risk Source:
Risk Source is an element which alone or in combination has the intrinsic potential to give rise to risk.

Risk Tolerance / Risk Appetite:
Risk Tolerance or Risk Appetite is the driver of Risk Strategy of an organization. It defines the maximum quantum of risk which the company is willing to take as determined from time to time in consonance with the Risk Strategy of the company.

Risk Description:
A Risk Description is a comprehensive template covering a range of information about a particular risk that may need to be recorded in a structured manner. It is an input to the Risk Register.

Risk Register:
A 'Risk Register' is a tool for recording risks encountered at various locations and levels in a standardized format of Risk Description. It becomes a major input in formulating subsequent Risk Strategy.

Likelihood:
Likelihood means the chance of something happening; whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively and described using general terms or mathematically such as a probability or a frequency over a given time Period.

Risk Profile:
Risk Profile is a description of any set of risks that may relate to the whole or part of the organization or as otherwise defined.

Risk Analysis:
Risk Analysis is a process to comprehend the nature of risk and to determine the level of risk. It provides the basis for Risk Evaluation and decisions about Risk Treatment, including Risk Estimation.

Risk Criteria:
Risk Criteria is a term of reference against which the significance of a risk is evaluated. They are based on organizational objectives and external or internal context and can be derived from standards, laws, policies, and other requirements.

Risk Evaluation:
Risk Evaluation is a process of comparing results of Risk Analysis with Risk Criteria to determine whether the risk and / or its magnitude is acceptable or tolerable. It assists in the decision about Risk Treatment.

Risk Treatment:
Risk Treatment is a process to modify a Risk. It is also referred to as 'Risk Mitigation,' 'Risk Elimination,' 'Risk Prevention' and 'Risk Reduction.' It can create new risks or modify existing risks.

Control:
Control is a measure of modifying risk and includes any process, policy, device, practice, or other actions which modify risk. It may not always deliver the intended or assumed modifying effect.

Residual Risk:
Residual Risk is a risk remaining after Risk Treatment. It can also contain unidentified risk and be known as 'Retained Risk.'

Owner: Risk Management Team
Month of Review: April 2023

****