ANNEXURES

INDEX

ANNEXURE 1: RISK MANAGEMENT FRAMEWORK (RMF) FOR MUTUAL FUNDS[1]

1.0 RMF Standards

i. AMCs shall establish a RMF for its mutual fund business. The RMF of mutual funds shall have the following characteristics:
   a. Be structured, efficient and timely.
   b. Be an integral part of the mutual fund's processes and governance framework, at both the operational and strategic level, and consider all available information i.e. both internal and external.
   c. Be customized to both AMC's and scheme's risk profile, focuses on potential risks and implements mitigation and control measures to explicitly address uncertainty.
   d. Be dynamic and flexible enough to identify new risks that emerge and make allowances for those risks that no longer exist.
   e. Recognize that people and culture have an impact on its effectiveness, and accordingly the framework must communicate and consult with stakeholders throughout.
   f. Protect reputation.

ii. The objectives of RMF should assist the management and the Board of Directors of both AMC and Trustees in:
   a. Demonstrating high standards of due diligence in daily management.
   b. Promoting proactive management and early identification of risk.
   c. Assigning and increasing accountability and responsibility in the organization.
   d. Managing risk within the tolerance limits defined in the RMF.

[1] SEBI/HO/IMD/IMD-1 DOF2/P/CIR/2021/630dated September 27, 2021

iii. The RMF of mutual funds shall comprise the following components:

a. Governance and Organization.

b. Identification of Risks.

c. Measurement and Management of Risks.

d. Reporting of Risks and related Information.

1.1 Governance and Organization

i. Risk Management shall be an independent and specific function of the AMC.

ii. There should be at least one CXO level officer identified to be responsible for the risk management of specific functions of the AMC/Mutual Fund. For instance, there should be dedicated risk officers for various key risks such as Investment Risk (by Chief Investment Officer), Compliance Risk (by Chief Compliance Officer), Operational Risk (by Chief Operating Officer or similar functionary responsible for the respective functions overseen), Cyber Security (by Chief Information Security Officer), etc.

iii. The policy on risk management of the mutual fund should have clarity on roles and responsibility assigned to CXOs and the same needs to be disclosed on their website.

iv. AMC should have a Chief Risk Officer (CRO), who would be responsible for the overall risk management of the mutual fund operation including the key risks. This is in addition to one CXO level officer responsible for each key risk type. The CXO shall be the "Head of Department" or official of the AMC up to one level below CEO, other than CRO. However, for the overall risk management of the mutual fund, along with the management, both board of AMC and trustees should also be responsible. For this purpose, both the AMC and the trustees should mandatorily have separate Risk Management Committees (RMCs). These

committees shall undertake annual review of RMF at both AMC and scheme level. The CRO should be part of the RMCs. The RMCs shall report to the Board of AMCs and trustees respectively and also recommend long term solutions regarding risk management both at the AMC level as well as the scheme level.

v. There shall be clear demarcation between the roles and responsibilities of the respective CXOs and the CRO. For instance, while defining the role of CRO, it should be ensured that the CRO would be responsible for the overall governance of the RMF; the investment decisions and the other functions of CIO are not encroached upon and the risk taking ability of CIO in accordance of the scheme objective is not hindered. The CRO or the risk management function of the CRO cannot be entrusted with day to day functioning, the responsibility for which shall lie with the respective CXOs.

vi. The AMC should maintain risk metric for each mutual fund scheme. The risk metric should incorporate each key risk type like investment risk, liquidity risk, credit risk, etc. along with the path to maintain the targeted risk level. The metric may incorporate evaluation of risk levels vis-à-vis an appropriate benchmark, wherever applicable. The RMCs shall meet at least once in a quarter to review various risks including risk metrics at both the scheme and the AMC level and assist the board of AMCs and trustees in discharging their duties in this regard.

1.1.1 Risk Management Policy

The risk management policy can be a macro level description of risk management governance (including roles and responsibilities of the Board of AMC and the three lines of defense – *Management, Risk Management*

Team and Internal Auditor), the organization's risk appetite and key elements of its risk management process. The policy on the RMF shall be approved by the board of AMC and trustees. The mandatory and recommendatory elements for inclusion in the risk management policy, approved by the board of AMC and trustees, are outlined below:

1.1.1.1 Mandatory Elements

i. There shall be an approved policy on the RMF both at AMC and scheme level.
ii. A risk appetite framework should be in place at both AMC and scheme level. Quantification of the framework in the form of a metric for key risks shall include but not limiting to credit risk, market risk and liquidity risk, etc. and targeted path of improvement. The metric, wherever applicable, should incorporate an appropriate benchmark vis-à-vis which the measurements of risk and targeted risk levels may be made.
iii. There should be a Delegation of Power (DoP) framework covering daily risk management, daily risk reporting and corrective actions at various levels of management.
iv. Formation of RMCs (of both AMC and Trustees), its roles and responsibilities.
v. Each CXO level officer to take ownership of risks and manage risk level for those risks as are applicable to their area of operation.
vi. Clarity on roles and responsibility assigned to CXOs
vii. Responsibility of line management and process ownership for risk management and reflection of the same in the performance appraisal through Key Result Areas (KRAs) of key officials of line management. The performance may be evaluated vis-à-vis an appropriate benchmark, if applicable.

viii. All aspects of risks that the AMC can face along with the mitigation plans, including but not limited to:
   a. Risk management practices in fund management, customer service, marketing and distribution.
   b. Disaster recovery and business contingency planning.

ix. Limit management framework for the material or key risks.

x. Risk assessment & monitoring measures and tools for all risks with quantified risk indicators and limits thereto.

xi. Implementation of scenario analysis and stress testing.

xii. Risk mitigation requirements and control mechanisms.

xiii. Additional triggers that could require review of the RMF, including:
   a. Material claims or litigations from customers or incidents.
   b. Material findings from internal or external audits.
   c. Adverse media attention impacting reputation risk.
   d. Adverse observations from the regulator(s), etc.
   e. Key risk indicator breaches.
   f. New regulatory requirements.
   g. Sector-relevant developments or incidents.

1.1.1.2 Recommended Elements

i. Use of technology to automate risk management, reporting and compliance.

1.1.2 Risk Management Function – Responsibility of Board of AMC, Trustees and the Management

1.1.2.1 <u>Risk Management - Role of the Board of AMC and Trustees</u>

i. Approving the RMF policies and procedures including the risk metrics at scheme level.

ii. Defining, reviewing and approving the AMC's and scheme's risk appetite framework.
iii. Periodic monitoring of risk appetite versus actual risk at scheme level.
iv. Event based monitoring of Risk appetite versus actual risk at scheme level.
v. Define specific responsibility of the management, including CEO
vi. Approval for policy for risk based KRAs and KRAs at level of CEO and up to one level below CEO. Suggest modifications in KRA outcomes and link compensation to those KRAs.
vii. Review of actions taken by Board of AMC and management in respect of risk management.
viii. Reporting of material risk related observations to SEBI on periodic basis.
ix. Setting up of the risk management function and developing appropriate structures and procedures to ensure that it can function independently.
x. Approving a methodology for Board Evaluation of the RMF (either through outsourced or self-assessment) on an annual basis.
xi. Annual review of effectiveness of the AMC and/or management's risk management function and policies including risk metrics to address the risk outcomes.
xii. Trustee may recommend reduction/ change in the risk level of the schemes within the Potential Risk Class (PRC).
xiii. For assessing the effectiveness of the RMF,

    a. The board of AMC should seek an annual report through an internal management assessment process or from a third party covering all key risks and key risk metrics both at the AMC and scheme level.

b. The RMCs of both AMCs and Trustees shall meet at least once in a quarter to review various risks including the risk metrics at both AMC and scheme level.
c. The Board of AMC should have all relevant information of appropriate committee(s) (with the mandate and membership), CRO, CXO(s) for specific risk management, audit functions, investor relations, investment and credit decisions, etc.

1.1.2.2 Risk Management - Role of the Management

i. The risk management role of the management can be broadly classified into risk management roles and responsibilities of the CEO, CRO, CIO, CXOs and the fund manager.
ii. The overall role of the management shall be as below:
    a. Overseeing the risk management function.
    b. Keeping the Board of AMC and Trustees informed on new or emerging risks.
    c. Putting in place a mechanism for risk reporting on quarterly basis to the Board of AMC and trustees, covering all risks including risk metrics, escalation of material risk related incidents, if any, and timely and corrective actions taken in specific cases of risk escalation. This may be carried out with an objective to address the root cause in escalation of such risks and also to improve the measurement and control mechanism for prevention of reoccurrence of such risks.
    d. Establishing an organization-wide risk-conscious culture.
    e. Inclusion of risk management as a parameter for performance appraisal (through KRAs or equivalent) of all the officials of the AMC at the level of CEO and up to two levels below CEO.

f. 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.

1.1.2.2.1 Risk Management - Role of Chief Executive Officer (CEO)

i. The CEO shall be responsible for all the risks at both AMC and Scheme level.

ii. The CEO shall

   a. ensure that the outcomes of risk management function are reported to him on a monthly basis

   b. define specific responsibility of CIO and CXO regarding risk management

   c. define a risk appetite framework for schemes and AMC.

   d. define appropriate risk metric for respective CXO, CIO, fund manager, etc.

   e. 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.

   f. The CEO shall approve the corrective action on various findings and report to the board of AMC and trustee regarding the same and also escalate to board of AMCs and trustees, if required, any major findings being reported.

1.1.2.2.2 Risk Management - Role of Chief Risk Officer (CRO)

i. 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.

ii. The risk management 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.

   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:

      1) Daily risk management

      2) Daily risk reporting

      3) Corrective actions at the level of Fund manager, CIO and CEO.

   h. The CRO shall inform to 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.

1.1.2.2.3 Risk Management - Role of Chief Investment Officer (CIO)

i. Daily management of risk and necessary reporting relating to Investment risk of all scheme(s) such as market Risk, liquidity Risk, credit risk etc. and other scheme specific risks (Compliance Risk, Fraud Risk, etc.) lies on the CIO.

ii. In respect of all schemes CIO should ensure:
   a. 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.
   b. Defining specific responsibility of Fund Managers
   c. Adherence to risk appetite framework - maintain risk level for schemes

iii. CIO will 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 risko-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.

iv. The CIO shall escalate the corrective actions taken, if any, to the CEO and the CRO.

1.1.2.2.4 Risk Management - Role of other CXOs

i. The CXOs shall be responsible for the governance of the respective risk types.

ii. In respect of respective risk type, CXO should ensure:
   a. 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.
   b. Defining specific responsibility regarding risk management of key personnel reporting to them.
   c. Maintaining risk level as per the risk metric.

iii. The CXOs shall take immediate corrective action for non-compliance or major finding post approval from CEO as per DoP and shall report to CRO regarding the risk reports.

iv. The CXO shall escalate to CEO and the CRO any major findings reported by respective risk management function.

1.1.2.2.5 Risk Management - Role of Fund Manager (FM)

i. The FM shall be responsible for daily management of investment risk of managed scheme(s) such as market Risk, liquidity Risk, credit risk and other scheme specific risks and appropriate risk reporting of any risk related event to CIO.

ii. In respect of schemes managed by them, FMs should ensure:
   a. Adherence to relevant SEBI guidelines in respect of RMF and relevant principles thereunder including risk identification, risk management, reporting and corrective actions etc.
   b. Adherence to risk appetite framework to maintain appropriate risk level for schemes.

c. If there is any need of change in the risk appetite of the scheme within the PRC of that particular scheme, the same is to be with the approval of the CIO.

iii. The FM shall take corrective action, if required, as per the approved DoP and escalate major risk related event to CIO.

1.2 Identification of Risks

For the identification of risks, the RMF should address the following key questions:

1.2.1 What are the different types of risks faced by the mutual fund/AMC and its mutual fund schemes?

1.2.2 What is the probability of the happening of each of the above risks, considering the control environment and automation within the AMC, external factors or dependencies such as market infrastructure, outsourced activities, etc. and available historical risk data?

1.2.3 What is the likely impact of key risk events, in terms of financial loss, reputation loss, impact on investors/ unit holders and regulatory action?

1.2.4 What are the emerging or new risks due to new business lines, new products, statutory changes, changes in external environment or market infrastructure, etc.?

1.2.5 The mandatory and recommendatory elements for identification of risks, are outlined below:

1.2.5.1 Mandatory Elements

i. Each AMC shall identify on an ongoing basis, the specific risks to be covered within the RMF, based on the nature, scale and

complexity of its business, the risk profiles and strategies of the funds it manages, and the impact of different risks on its mutual funds business.

ii. Documented risk profile for each of the key functions incorporating events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives, sources of risks and areas impacted due to the event.

1.2.5.2 Recommendatory Elements

i. Formalized risk appetite statement (incorporating themes such as investment, sales, and operational losses as a result of in-house or outsourced activities) both at the scheme and AMC level.

1.3 Measurement and Management of Risks

1.3.1 AMC should have approved internal policy for measurement of various scheme specific risks (such as governance risk, investment risk, liquidity risk, credit risk) through appropriate risk metrics.

1.3.1.1 It should reflect the Risk-O-Meter and the PRC of the scheme vis-a-vis the scheme benchmark.

1.3.1.2 The policy should have the defined guidelines regarding the appropriate risk metric with role clarity depending on the responsibility of each person.

1.3.2 AMCs should have approved internal policy for measurement of organization wide risk like operational risk, technology risk, legal risk, talent risk, outsourcing risk, etc.

1.3.3 Having identified and documented the applicable risks, the risk management function should develop process/tools to measure and

manage those risks. For this purpose, the following needs to be considered for each risk category:

i. Ascertaining the measurement criteria for each risk category (qualitative and quantitative criteria).
ii. Documentation of measurement tool(s) for each risk category, i.e. Risk and Control Self-Assessment (RCSA), stress testing, scenario analysis, etc.
iii. Determination of required frequency of monitoring.
iv. Developing a process for escalation.
v. Determination and documentation of remedial or mitigating actions.

Wherever appropriate, it is recommended that AMCs consider documenting risk limits based on their risk appetite.

1.3.4 The mandatory and recommendatory elements for measurement and management of risks, are outlined below:

1.3.4.1 Mandatory Elements

i. The AMCs shall have established structure and responsibility across the three lines of defense:
   a. Business Operations.
   b. Oversight functions like Risk Management and Compliance.
   c. Internal Audit.

ii. Internal Audit and Oversight functions like Risk Management and Compliance shall ensure the following:

a. There should be a dedicated internal auditor at the AMC level for audit of the RMF of the AMC.

   However, the same may be carried out by independent auditor appointed by trustees, provided that the personnel undertaking the said audit have relevant expertise in the domain of risk management necessary for both the AMC level and the scheme

level audit. In such scenario, care must be taken that no conflict arises w.r.t submission of independent audit reports by the auditor to the audit committee and the Board of both the AMC and the trustees for the conduct of their respective audit functions.

b. The internal auditor should audit both the scheme level and AMC level risks.
c. The internal auditor should audit compliance with the internal policies of the AMC on risk management as well as the applicable rules and regulations mandated by SEBI on risk management.
d. For the processes being audited by the internal auditor, a noncompliance rate shall be computed. The non-compliance rate may be computed based on sampling out of the total number of processes being audited.
e. The internal auditor should submit the internal audit report to the audit committee of the AMC and the Board of AMC representing the noncompliance rate as audited in the books of accounts of the AMC and its schemes. While submitting to the audit committee, the noncompliance level shall be converted to an overall internal audit score represented in the form of a number providing a quantitative representation of the internal audit report. This number shall be generated considering all key risk types.
f. Further, this number shall be compared in subsequent internal audits to analyze the improvement in minimizing the non-compliance level at the AMC. This shall reflect the degree of rectification of noncompliance as done at the level of AMC. Therefore, this number may be represented in the form of a "Rectification Index" in the internal audit report.

iii. There shall be an RCSA process with defined frequency.

iv. There shall be an established mechanism for reporting to the CRO, management and the Board of AMC and Trustees.

v. Periodic review of policy frameworks shall be done to ensure that the said policies are up-to-date responding to new strategic priorities and risks and the monitoring mechanisms are working to ensure compliance with the updated policies.

vi. Mechanisms are established for management to make use of early warning indicators to identify, evaluate, and respond to changes quickly.

vii. Periodic stress tests are performed on critical risks and the impact of risks are assessed based on acceptable tolerances.

viii. Based on the management of the risk level as defined by respective risk metric of CXOs, necessary corrective actions must be taken to address any short comings. The output of the risk level shall be an indicator of the performance of the respective CXOs and shall form one of the inputs for their performance review.

1.3.4.2 Recommendatory Elements

i. There should be independent testing and verification of efficacy of corporate governance standards and business line compliances, validation of the RMF and assurance over the risk management processes by external agency.

1.4 Reporting of Risks and Related Information

1.4.1 Adequate risk reporting is an integral part of the risk management framework and it is important that those responsible for different functions within the AMC shall ensure that they exercise sufficient

oversight to report on their risk profile and risk management actions.

1.4.2 The mandatory elements for reporting of risk and related information, are outlined below:

1.4.2.1 Mandatory Elements

i. In order to ensure that the risk management function obtains the necessary information from other departments as well as from outsourcing partners (wherever applicable), a structured bottom-up reporting process should be designed and the risk management function should perform meaningful and independent analysis of such information.
ii. The outcomes of the risk management function should mandatorily be reported to the management at least once on a monthly basis and to the Board of AMC and Trustees on a quarterly basis. Trustees may forward the results and steps taken to mitigate the risk along with their comments to SEBI in the half-yearly trustee reports.
iii. Risk reports should consider the following:
    a. It should be holistic (considering all risk categories identified), timely and accurate.
    b. It should incorporate the risk metrics comprising the risk profile of all schemes and the risk profile consolidated across the departments and the AMC level. It should also incorporate the rectification index as calculated in the internal audit report for both the AMC and the scheme level.
    c. It should contain all necessary information to assess whether appropriate measures have been taken by the management to control and mitigate all relevant risks.

d. It should provide information on existing as well as new risks including a statement on severity (e.g. low, medium, high) and its evolution over time, and the measures to mitigate existing risks where possible.

iv. The Risk management function shall ensure that any significant emerging risk issues that are not adequately addressed by the responsible functional department are promptly reported to the management or the risk management team and to the Board of AMC.

2.0 Managing Key Risks

a. SEBI (Mutual Funds) Regulations, 1996 vide various circulars has prescribed certain norms which would cover many aspects of risk management such as, stress testing, internal credit risk assessment, cyber security and system audit, liquidity buffer, creation of segregated portfolio, investment restrictions, investment due diligence, etc. that are to be adhered to by the mutual funds. The following sections incorporate comprehensive guidelines for management of various key risks by the AMCs, elements of which may overlap with the above mentioned norms and in such cases, the detailed norms specified in the relevant circular must be strictly followed.

b. These key risks may be divided in to two broad categories.

   i. Scheme specific risks

   ii. AMC specific risks

c. The scheme specific risks are the risks majorly associated with the core activities of investment and portfolio management. The AMC specific risks are the risks associated with the functioning of the mutual fund business by the AMC.

d. The scheme specific risks may be divided in to the following categories.

   i. Investment risk

   ii. Credit risk

   iii. Liquidity risk and

   iv. Governance risk

The AMC specific risks may be divided in to the following categories.

   i. Operational Risk

   ii. Technology, Information Security and Cyber Risk

   iii. Reputation and Conduct Risks

   iv. Outsourcing Risk

   v. Sales and Distribution Risk

   vi. Financial Reporting Risk

   vii. Legal & Tax Risks and

   viii. Talent Risk

The compliance risk shall be applicable for both investment management activity (scheme specific risk) and business activity of AMC (AMC specific risk).

The following sections incorporate comprehensive guidelines for management of the key risks

2.1 Investment Risk

2.1.1 Investment risk can be defined as the probability or likelihood of occurrence of losses relative to the expected return on any particular investment.

2.1.2 Investment risk management should be based on reasonable investor expectations about the risks that the mutual fund will take in order to achieve its investment objectives, which can be thought of as the fund's risk profile or risk appetite. A fund's risk profile should be stated in its communications with investors including in its Scheme Information Document (SID) and marketing materials, which state the fund's investment strategies and risk factors. The SID shall also incorporate any other elements of risk appetite as may be stipulated by AMCs and Trustees.

2.1.3 Investment risk management should involve both controlling risk by limiting certain risk exposures and the size & probability of losses, as well as using a number of active investment techniques that seek to align the fund's investments with its investment objectives, its risk profile, and the portfolio manager's investment convictions.

2.1.4 Risk control should focus on placing limits on a fund's investment positions and concentrations. These limits should include the investment restrictions mentioned in the fund's SID as well as any limits and restrictions imposed by the risk management function within the regulatory limits. Risk control activities may include reviewing portfolio concentrations and adjusting portfolio holdings accordingly; evaluating and reviewing new and/or complex instruments, such as derivatives, and imposing conditions and limits on their use; monitoring and limiting credit exposure from issuers of portfolio securities and from counterparties; and ensuring that a fund is managed in compliance with the SID and the regulatory investment restrictions.

2.1.5 The mandatory and recommendatory elements for managing investment risk, are outlined below:

2.1.5.1 Mandatory Elements

i. The AMC should have the following policies / process:
   a. An investment universe to be updated periodically and responsibility for the same should be clearly defined.
   b. An investment policy for investment in various asset classes/ securities as permitted by SEBI from time to time and policy on hedging of interest rate risk, foreign exchange risk, price risk, etc.
   c. Policy on participation in IPOs/FPOs including policy on participation in IPOs/FPOs of associate/ group company(ies).
   d. Trade execution policy.
   e. Policy on trade allocation and Inter-Scheme Transfers (ISTs).
   f. Investment valuation policy.
   g. Broker empanelment policy.
   h. Trustee should review the portfolio at frequency as required by SEBI Regulations.

ii. The AMC must ensure that investment risk is adequately factored in by:
   a. Setting up an Investment committee which has close coordination with related departments, and monitors market risk.
   b. Setting limits for issuer/ sector exposure vis-a-vis benchmark (in line with MF Regulations and internal limits).
   c. Setting limits for investment in debt and money market instruments of various credit qualities.
   d. Having all relevant documents and disclosures (that are required for listing) with regard to the debt and money market instruments before finalizing the deal for investment into the respective instruments so that mutual funds as investors into such

instruments are not at an informational disadvantage vis-à-vis other market participants or lenders.

e. Review of passive breaches and corrective actions.

iii. Investment Committee shall be responsible for the following:

a. Review of Investment Policy at a pre-defined frequency.

b. Reviewing the Investment plan or policy to meet the investment objectives documented in the SID.

c. Any other responsibility as assigned by the management.

iv. The AMC should conduct the following to manage and monitor investment risks (at scheme level or aggregate portfolio level, whichever is applicable):

a. Redemption analysis.
b. Investor concentration analysis. Both single investor and/or group concentration.
c. Monitor investment risk at a defined frequency.
d. Managing and monitoring investment restrictions for overseas investment, if any.
e. Monitor investment risk at individual portfolio level and also concentration risk and other relevant risks at aggregate level in a structured manner.
f. Stress testing for investment risk.
g. Consider investment risk while launching new products.
h. Ensure that Trade Allocation policy is adhered to along with adequate information to identify those allocations that are out of line with the normal percentage allocation across funds.
i. Quantitative risk analysis using metrics such as VaR, Sharpe Ratio, Treynor Ratio, Information Ratio, etc.

j. Prepare and maintain management reports on topics discussed and conclusions made at investment committee meetings (including interest rate prospects, risk-taking and hedging policy, etc.)
k. Distributor concentration analysis.

v. Further, it should be ensured that:

a. Actual risk measures and reports are adapted to the risk characteristics of the individual asset classes, and capture dependencies between risks (e.g. market risk and liquidity risk).
b. Actual risk measures address risks in normal and stressed market conditions.
c. Actual risk measures cover all risk types in the portfolio, including counterparty credit and liquidity risks (assets, investors).
d. Appropriate tools are adopted for measurement of market and credit risks on different types of investment products.
e. Adequate processes and controls are in place to ensure that risk reporting is complete, accurate, timely and meets the needs of various stakeholders.
f. Adequate documentation of calculations, analyses and decisions is maintained.
g. Performance and positions with regard to objectives of schemes are reviewed.
h. Performance vis-à-vis scheme benchmarks and performance of peer group(s) is reviewed.
i. Exceptions are defined and their monitoring is conducted.
j. Exceptions in style drift and portfolio concentration are reviewed.
k. In cases of inter scheme transfer, the scheme (s) buying the securities must conduct an enhanced level of due diligence.

2.1.5.2 Recommendatory Elements

The AMCs may consider the following practices:

a. Regular analysis on bulk trades and block deals of large values.

b. Formulating a plan for assessing and monitoring risks of investing in multiple markets.

c. Setting limits for minimum number of stocks/securities, cash (net of derivatives), stocks/securities vis-a-vis benchmark and Beta range.

2.2 Credit Risk

2.2.1 The credit risk relevant to mutual funds is the issuer credit risk attributable to individual securities and the negative outlook on specific sectors or industries and its consequent impact on the credit exposures.

2.2.2 The mandatory and recommendatory elements for managing credit risk, are outlined below:

2.2.2.1 Mandatory Elements

i. To manage credit risk, the AMC must have a robust framework comprising:

   a. An approved and documented Credit Risk Management policy.

   b. Analysis and evaluation of ratings received from multiple credit rating agencies for securities across portfolios, at all points of time i.e. before investing in such securities/instruments or products and also on continuous basis.

c. Formal procedure for AMCs to carry out their own credit assessment of assets and reduce reliance on credit rating agencies. For this purpose, all AMCs shall have an appropriate policy and system in place to conduct an in-house credit risk assessment or due diligence of debt and money market instruments or products at all points of time i.e. before investing in such instruments or products and also on continuous basis.

d. Adequate provisions to generate early warning signals (including yield based alerts) on deterioration of credit profile of the issuer. Based on the alerts generated, the AMCs shall take appropriate measures and report the same to trustees.

e. Concentration limits (counterparty wise, group wise, industry or sector wise, geography wise) monitoring.

f. Stress testing for credit risk - applying shocks based on rating downgrades, negative outlook on specific industries and the consequent impact on credit exposures.

2.2.2.2 Recommendatory Elements

i. Over a period of time and having regard to the size, scale and complexity of the fixed income portfolio, AMCs may consider developing sector level standards for implementing internal credit assessment based models to measure credit risk in line with the prevailing global best practices.

2.3 Liquidity Risk

2.3.1 Thinly traded securities carry the danger of not being easily saleable at or near their real values. Further, all securities run

the risk of not being saleable in tight market conditions at or near their real values. Measuring and monitoring liquidity risk is an important aspect of risk management.

2.3.2 The mandatory and recommendatory elements for managing liquidity risk, are outlined below:

2.3.2.1 Mandatory Elements

i. Liquidity Risk has to be modelled at the level of each scheme (except schemes that do not have continuous liquidity requirements like close ended and interval schemes) and should display alerts pertaining to asset liability mis-match on monthly basis and in line with any other relevant guidelines as specified by SEBI in this regard from time to time. The aforesaid model, should be based on the following key principles:
   a. The secondary market liquidity of assets of the scheme, shall be incorporated into the liquidity risk management model.
   b. For debt and money market instruments, the total asset value shall be classified in various maturity buckets for e.g. assets maturing in days 0-30, 30-60, 60-90 and so on. Debt and money market instruments that have a demonstrable secondary market liquidity shall be classified into a lesser maturity bucket depending upon the reasonable time in which particular value of the said instrument can be expected to be offloaded. In the absence of demonstrable secondary market liquidity, the instruments shall be strictly classified based only on the maturity dates.
   c. Liabilities of scheme shall be modelled in similar buckets based on back testing of historical data for subscription and redemption amounts in the respective schemes. The back testing period should be sufficiently long (say for last 5 years) to include spikes

in redemptions because of market wide events. Organization specific factors/risks that may have a bearing on redemptions should also be factored into the model.

d. Liquidation of assets at near the value ascribed to each asset in the scheme portfolio in specified period of time, shall be one of the factors to be considered in liquidity risk management.
e. The model should incorporate forward looking asset liability mis-match for the scheme at different periods of time at least up to next 30 days.

ii. The AMC should have policy in place on management of the mis-match in putative liabilities vis-à-vis the liquid assets of each scheme. It should follow the following principles:
    a. There should be an upper limit or threshold on the mis-match in putative liabilities vis-à-vis the liquid assets of each scheme. The upper limit shall be customized depending on size or type of the scheme.
    b. There should be a system based mechanism to generate alerts as per point(a) above.
    c. The policy shall include monthly reporting to Board of AMC and Trustees and on quarterly basis to SEBI in a standard format (to be prescribed by AMFI in consultation with SEBI).
    d. The report shall include the details of alerts generated by the system regarding asset liability mis-match in excess of the defined threshold and subsequent actions taken to address the same. The scheme wise mis-match limits shall be put in the system and all alerts shall be managed effectively.

iii. Stress testing should be mandatorily conducted for all schemes (excluding close ended and interval schemes) appropriately atleast on

monthly basis. The results of the stress testing may be placed before trustees in every quarter. Trustees may forward the results along with their comments and steps taken, if any, to SEBI in the half-yearly trustee reports. With respect to stress testing of open ended debt schemes, norms have been provided under Paragraph 4.2 of the Master Circular and the same must be adhered to and any future guidelines issued by SEBI in this regard may suitably be followed.

iv. The policies and procedures implemented by the AMC should include the following:
    a. Measures and limits for monitoring liquidity risk - cash flow approaches, ratios/tools for monitoring market liquidity (including equity market), etc.
    b. Measures for managing intra-day liquidity and controls around the same.
    c. Stress testing policy to align the stress testing requirements mandated by SEBI for mutual funds in India specifically incorporating:
        1. Risk parameters used and methodology adopted to conduct the stress tests.
        2. Procedure to deal with stress events and early warning signals.
    d. Overview of funding plans/strategy during normal and stressed events, including contingency funding plan.

v. Systematic classification and evaluation of liquidity risks should be initiated by performing following activities:
    a. Evaluation and disclosure of liquidity risk associated with schemes/products in the SID.
    b. Controls around preparation and accuracy of cash flows.

c. Management of collateral and margins for execution and settlement of derivatives, securities and money-market instruments.

2.3.2.2 Recommendatory Elements

i. AMCs may consider introducing the following measures:

a. Judicious use of intraday / overnight borrowing lines to address liquidity / settlement risks faced by the mutual funds. Uncommitted lines of credit available with the AMC may not be useful in real time of stress and therefore while assessing liquidity risk of AMC, these lines should be treated differently than committed lines.
b. Internal committee with the mandate to review and provide direction on liquidity risk management.
c. Identifying and reporting appropriate and relevant information to the management, for decision making.
d. Reporting to the Board of AMC on any other material outcomes and events.

2.4 Governance Risk

2.4.1 Governance risk is a risk that the persons who are in position of power or fiduciary responsibility towards the holders of security (equity/debt), do not act in the best interest of such stakeholders, rather compromise the interest of such stake holders for their personal gain.

2.4.2 The act of people with power may significantly impact the equity market price of the shares along with having a direct impact on debt issuances.

2.4.2.1 Mandatory Elements

a. The AMC shall have an approved policy to deal with governance risk of the investee companies.
b. The policy shall incorporate measures such as assessment of whether there are enough system checks and balances in the governance structure of the issuer to prevent such wrong doing and also assessment of track record or history of the issuer to monitor the trend of their past behavior.
c. The policy shall also include guidelines on how it identifies and monitors any conflicts of interest involving members of the Board/ KMPs of the investee company.
d. The AMC shall adhere to the "Stewardship Code" prescribed by SEBI for mutual funds which inter alia includes continuous monitoring of the investee companies on various matters such as operational and financial performance, corporate governance, related party transactions, opportunities or risks including ESG risks, etc., bearing in mind the insider trading Regulation while seeking information from the investee company for the purpose of monitoring etc.

2.5 Operational Risk

2.5.1 Operational risk refers to the risk of loss resulting from inadequate or failed processes, people and systems or from external events, e.g. internal fraud, external fraud, physical damage caused by nature or man-made, etc.

2.5.2 As operational risk could manifest in any function or process within the organization or at a third party service provider, it is important to have adequate monitoring and tracking of all elements that can

go wrong. This includes fails, reconciliation differences, customer complaints, guideline breaches, systems issues, process gaps, system bugs, etc. It is equally important to have an escalation process as any undue delay in reporting could magnify the loss or turn a gain into a loss.

2.5.3 The key for effective operational risk management should be to create a process that tracks the various elements of operational risk over time, to identify trends that could be an early warning signal, and to implement an exception/escalation process that ensures the problems which are significant, large, aged or growing dealt with at increasingly higher levels of management.

2.5.4 Paragraph 6.15 of the Master Circular has provided indicative guidelines encompassing system audit framework. The systems and processes as elaborated in the aforementioned paragraphs must be in place and any future guidelines issued by SEBI in this regard may be suitably followed.

2.5.5 The mandatory elements for managing operational risk, are outlined below:

2.5.5.1 Mandatory Elements

i. The AMC should implement the following policies:

a. Operational risk management policy, shall cover the following key elements:

1. Purpose and scope.
2. Governance Structure - Roles and Responsibilities.
3. Identification of operational risk events.

4. Management of the operational risk events, e.g. reversal of positions, rectifications, etc.
5. Guidelines regarding transactions with associates, group entities, related parties or even with other stakeholders, such as distributors, channel partners, brokers, etc.
6. Escalation and reporting.
7. Compensation of loss, if any.
8. Follow-up actions, e.g. strengthening of systems and processes, training, etc.
9. Communication with external stakeholders - regulators, investors, distributors, etc.
10. Implementation of a 'new product approval' process to ensure that all functions have the systems, people, processes to support a new product
11. Recording and documentation.

b. The Dealing room policy incorporating the non- usage of mobile, restricted internet access, dedicated recorded lines, handling of information, etc. In this regard, the detailed guidelines on this aspect as provided in Paragraph 12.29 of the Master Circular as well as in the part B of Fifth Schedule of SEBI (Mutual Funds) Regulations, 1996 or any further SEBI guidelines may be referred to.

c. Roles and responsibilities are defined for the following:
    1. Time stamping, application processing and confirmation,
    2. Review of KYC and investor declarations as specified through various SEBI regulations,
    3. Timely and accurate credit identification (for investor subscription) and bank reconciliations (banks/custody).

4. A system to track and report high value transactions (including bulk redemptions) to the Investment management function.
5. Control oversight on brokerage computation and payment, redemptions, inter-scheme switches, maturity payments in closed ended funds, dividend payouts, tax and other statutory payments, subscription refunds, identification of unclaimed amounts and their deployment as per regulatory requirements, etc.
6. Review of 'value dated' transactions, reversals, broker/ distributor code changes, etc.
7. Incident reporting and escalation matrix for the same.
8. Maintaining a Chinese wall between the different businesses earned out by the Asset Management Company (such as PMS, AIF, Overseas Investments, Advisory, Mutual Funds, etc.)
9. Documented process to review human errors in transaction processing to identify training needs and corrective actions to prevent the errors in the future.

d. There is an adequate RCSA process for operational risks on a periodic basis with a structured reporting methodology.

e. The AMC should perform the following:

1. Analyze and classify frauds into internal (within the organization) and external (by persons outside the organization) frauds, identify root causes and incorporate monitoring mechanisms to address fraud scenarios.
2. Reporting of frauds and near miss incidents to the Board of AMC and Trustees on quarterly basis.

f. Insurance cover shall be obtained for first and third party losses:

1. The mutual fund must have insurance cover against third party losses arising from errors and omissions:
   (a) Third party liabilities refer to liabilities arising out of financial loss to investors or any other third party, incurred due to errors and omissions of directors, officers, employees, trustees, R&T agents, custodians etc.
   (b) The level and type of cover should be recommended by the AMC and approved by the Trustees.
2. Further, the AMC shall have insurance to cover first party losses:
   (a) First party losses are those which impact the insured and include asset based losses (due to natural or unnatural disasters such as fire, flood, burglary, etc.) as well as financial or data losses.
   (b) They also include losses due to the acts of employees of the insured and computer based crimes such as hacking or virus attacks that may impact the data of the mutual fund, etc.
   (c) Key details of the same, together with claims thereunder, shall be annually reported to the Trustees.

g. The AMC should have an integrated system (front-mid-back) to perform the following functions:

1. Order generation
2. Position-keeping (Positions on all supported products are updated in real time). Trades can be accounted for by an electronic feed.
3. Pre-trade compliance checks
4. Order execution
5. Deal booking

6. Straight-through processing to allow one-time capture of trade details.
7. System check on preset parameters and reporting of breaches e.g. whether investments made in permitted securities or limits on deal size, etc. have been adhered.
8. Automatic time-stamping of deals.
9. Maker-checker authorisations.
10. Exception reporting.
11. Generation of deal confirmations.
12. Monitoring of outstanding confirmations, settlements and payments.
13. Cash management.
14. Integrated reporting across the Mutual Fund.
15. The back office system should facilitate daily fund projections to ascertain liquidity and settlement requirements.

h. The AMC should have documented procedures for the following:
1. Trade confirmations, settlements.
2. Cash flow Management.
3. Collateral Management.
4. Corporate Actions.
5. Margin Management.
6. Security Master Creation.
7. Pricing and Valuation.
8. Corporate action tracking and accounting.

9. Oversight on Service Providers – Custodians, Fund Administrators - SLA tracking, Parallel Valuation and calculation of NAV. The oversight over custodians shall inter alia include, receipt of daily position report from custodian, end of day reconciliation of positions with custodian data and once a week complete reconciliation of fund accounting system records with custodian records.

i. The AMC may implement the following depending upon the scale and complexity of business:

   a. Documenting a Fraud Response Plan and reporting of near miss incidents.
   b. Developing Fraud Risk scenarios and updating with changing business dynamics, documentation thereof being maintained in appropriately designed and updated Fraud Risk Registers (capturing details such as past fraud incidents).
   c. Using data analytics as a key tool for identifying fraud patterns and indicators.
   d. Conducting a fraud control and reporting' training program.

2.6 Compliance Risk

2.6.1 Failure by the AMC to meet its regulatory obligations or manage changes in legal statutory and regulatory requirements may result in investigations, fines, financial forfeiture, or regulatory sanctions and material loss to investors and the organization.

2.6.2 The mandatory and recommendatory elements for managing compliance risk, are outlined below:

2.6.2.1 Mandatory Elements

i. The AMC shall establish and maintain policies as required by applicable statutes and regulations, including policies to address the following:
   a. Know Your Client (KYC), Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT)
   b. Outsourcing
   c. Customer Complaints & Investor Grievance – Should inter alia include details of adherence to SEBI regulations with regard to investor servicing and complaint resolution, tracking complaint resolution, update of complaint log and forwarding of complaints and the Management Information System (MIS) to compliance officer, complaint resolution process being reviewed by compliance officer. The compliance officer shall review the complaints with an objective to catch early warning signs for fraud or any systemic issues.
   d. Related Party Transactions.
   e. Front running
   f. Conflict of Interest.
   g. Employee Trading (including issues related to Insider Trading).
   h. Code of Conducts.
   i. Commission and other sales & marketing costs.
   j. Commercial Bribes or Kickbacks.
   k. Fraud Risk Management
   l. Whistle Blowing
   m. Information Security and Data Privacy
   n. Gifts and Entertainment
   o. Record Retention
   p. Dealing Room Policy

q. All disclosure requirements (including derivative transactions, off balance sheet items and contingent liabilities, etc.).

ii. There should be defined responsibilities for:

a. Filing of timely and accurate regulatory reports to the Regulator(s) and Board of AMC and Trustees as prescribed by the applicable laws and regulations.

b. Pre-use review of AMC's marketing materials (collateral, brochures etc.), website uploads, digital advertising and performance advertising etc.

c. Monitoring that all investments and holdings are consistent with disclosures made to clients and applicable restrictions.

d. Mechanism for prevention or detection of possible insider trading at the personnel or portfolio levels.

e. Review for adequacy of disclosures made to the investors regarding significant risks such as liquidity, counterparty and credit (quality of investments made mainly debt based on the credit rating), investment, and other risk areas.

f. Measures to prevent and detect trading violations involving short selling.

g. Maintenance of all required licenses, registrations, approvals and permissions.

iii. AMCs should have an Anti-Money Laundering/Combating Financing of Terrorism (AML/CFT) program with the following attributes:

a. Employees understand obligations and contents of policies to effectively carry out their AML/CFT responsibilities.

b. Transaction Monitoring is done to identify Suspicious Activities.

c. Suspicious Transactions Reporting is done to the relevant authorities.

d. Adequate training programs to ensure employees are constantly aware of money laundering/financing of terrorism risks and measures (focus on their roles and responsibilities).

iv. AMCs should have systems in place to detect and prevent securities market violations including securities market frauds and malpractices at their end:

a. A report containing details of the alerts generated and the subsequent actions taken in this regard should be submitted to trustees on a quarterly basis.

b. Trustees may forward the results along with their comments and steps taken, if any, to SEBI in the half-yearly trustee reports.

2.6.2.2 Recommendatory Elements

i. The following policies may be incorporated by the AMCs depending on complexity and scale of operations:

a. Political Contributions.

b. Outside business activity policy.

ii. The AML/CFT program of the AMCs may include the following depending on the size and scale:

a. Investor awareness programs (literature or pamphlets or such) to educate clients about the AMC's AML/CFT obligations.

b. Review of client risk scoring model to ensure effectiveness of the AML/CFT program.

c. Independent or External review of AML/CFT policies to ensure their effectiveness.

2.7 Technology, Information Security and Cyber Risk

2.7.1 Given the huge dependence on technology, any system failure could trigger a variety of risks, e.g. operational risk, compliance risk. etc. Technology Operations should support processing and storage of information, such that the required information is available in a timely, reliable, secure and resilient manner.

2.7.2 Increasing disclosure requirements on public portals by AMCs required a focused approach towards data management. Digitalization and online platforms have given rise to need for effectively mitigating information security and cyber risks.

Paragraph 4.7, 4.8 & 6.15 of the Master Circular has provided indicative guidelines encompassing cyber security and cyber resilience framework and audit framework encompassing systems and processes for Mutual Funds/AMCs. The systems and processes as elaborated in the aforementioned paragraphs must be in place and any future guidelines issued by SEBI in this regard may be suitably followed.

2.8 Reputation and Conduct Risks

2.8.1 The risk of damage to the firm's reputation that could lead to negative publicity, costly litigation, a decline in the customer base or the exit of key employees and therefore, directly or indirectly, financial loss or revenue shrinkage.

2.8.2 Conduct risk is often defined as the risk to the delivery of fair customer outcomes or to market integrity.

2.8.3 The mandatory and recommendatory elements for managing reputation and conduct risk are outlined below:

2.8.3.1 Mandatory Elements

i. The management must look into reputation and conduct risks and inculcate their significance in the AMC culture by,
    a. Integrating reputation and conduct risk considerations into strategy setting and business planning.
    b. Establishing a crisis management policy (to minimize or neutralize negative publicity in the event of any incident or bad conduct by an employee).
    c. Establishing monitoring tool(s) for social media grievances, etc.

ii. The Board of AMC should approve and monitor the effectiveness of implementation of an enforceable code of ethics and business conduct; in the event of a material breach in conduct or a significant reputation risk event, the Board of AMC should be informed.

iii. The following practices must be adopted by the AMC:
    a. While designing or improving the products, the complexity of the product and consumer behaviors must be considered.
    b. Impact assessment should be undertaken for sales and promotion expenses (i.e. evaluation of value added v/s cost incurred) using appropriate techniques, e.g. analysis of complaints, compliance monitoring program, data analytics, mystery shopping, etc.
    c. Preventive measures and monitoring mechanism should be implemented to mitigate mis-selling risks.

2.8.3.2 Recommendatory Elements

i. AMCs may consider adopting:
    a. Reputation risk policy.

b. Media interaction policy and procedures
c. Assessment and management of reputation via brand management tools, data analytics, business intelligence.
d. Framework / Process to review and action any negative mention in traditional or social media.
e. Procedures to monitor reputation risk on an ongoing basis.

ii. The management may be involved in increasing awareness about conduct risk within the AMCs by:

a. Conducting training programs for conduct risk awareness.

b. Monitoring conduct risk indicators.

c. Incorporating conduct performance as part of the AMCs' sales and marketing team metrics.

2.9 Outsourcing Risk

2.9.1 Inadequate management of outsourced processes lead to errors, frauds, Inefficiencies, poor quality investor services, breach of fiduciary duties data pilferages and long term impact on reputation and contractual obligations.

2.9.2 Asset management companies often rely on third parties including Custodians, Fund Administrators, R&T agents, and various types of outsourced service providers who perform operational, accounting, recordkeeping and other types of services. In utilizing the services of such third parties, it is important from a risk management perspective to keep in mind that asset managers have ongoing fiduciary obligations to their customers even though they have delegated certain of their roles to others. It is therefore critical to perform careful reviews of the capabilities of third parties at inception of relationships and on an ongoing basis, and to review

information provided by third parties for completeness, balance and accuracy in order to be able to determine whether such third parties meet the risk management, credit, operational, legal and other relevant standards of the reviewing company with respect to the function they are performing.

2.9.3 The mandatory and recommendatory elements for managing Outsourcing risk, are outlined below:

2.9.3.1 Mandatory Elements

i. Risk management with respect to any outsourced activity should be done in the manner as if the activities were being done in-house.
ii. There shall be a dedicated person in the AMC who would be responsible for the outsourced activities of each outsourced vendor.
iii. The AMC should have a Board approved Outsourcing Policy incorporating the following aspects (as well as other applicable regulatory requirements):
    a. Listing of core activities which cannot be outsourced.
    b. Procedure for outsourcing, including risk and materiality assessment.
    c. Monitoring and control of outsourced activities (as part of outsourcing risk management program).
    d. Information security and confidentiality (including data privacy/ protection standards).
    e. Criteria for selection and minimum qualification.
    f. Minimum quality standards.
    g. Tenure of agreement.
    h. Responsibility for outsourced functions.
    i. Acceptable level of deviations.
    j. Periodic review of service levels and pricing.
    k. Restriction on sub-delegation or sub-contracting.

l. Right for inspection and audit.
m. Approval authorities.
n. Service level agreement.
o. Archival and retrieval of documents/data.
p. Insurance requirements.
q. Incident reporting and escalation matrix.

iv. Before outsourcing any activity, the AMC should ensure the following is in place:

a. Outsourcing agreements with service provider are legal and binding as per the law.
b. Due diligence (including AML/CFT, if applicable) is conducted on the service provider, where the outsourced activity is material, which may include the following considerations:
    1. Availability of qualified and experienced service providers to perform the service on an ongoing basis
    2. Arrangements for structured review of the capability and experience of service providers
    3. Evaluation of relevant personnel for critical functions, to evaluate their specific competencies and execution capabilities
    4. A disaster recovery and business continuity plan exist with regard to the contracted services and products, and that the adequacy and effectiveness of the same is maintained and tested periodically by the service provider.
c. Analysis of the benefits and risks of outsourcing the proposed activity as well as the service provider risk, and determination of the cost implications for establishing the outsourcing arrangement.

v. After outsourcing any activity, the AMC shall ensure:

a. Outsourcing vendors' process/people/systems are reviewed.

b. A periodic internal review is done on the functioning of outsourced activities (like Fund Accounting and R&T agent functions) at least annually.
c. An effective structured tool (IT / manual) is used to review/benchmark the performance of the third party service providers (Fund Administrators / Custodians / R&T agents) vis-a-vis the SLA.
d. The result of the review documented and risks emanating from them are highlighted and remediation plans are monitored on an ongoing basis.
e. Communication of its error tolerance, code of conduct and objective to its third party service providers (Fund Administrators / Custodians / R&T agents).
f. The service provider should test business continuity and contingency plan on a periodic basis to ensure adequacy and effectiveness'.

vi. The Mutual Fund should establish reconciliation procedures with regard to periodic reconciliation between fund accounting system, R&T system and bank account and conduct a periodic audit of all investor-related activities, carried out both by the Mutual Fund and the R&T agent, to ensure that all allotments, redemptions, income distributions and commission distributions have been accurate and timely.

vii. The Mutual Fund should ensure that the fund accounting systems used (inhouse or by the fund accountant to whom this activity has been outsourced) facilitate:
   a. Validation of NAV calculations.
   b. Automated and manual price feeds.
   c. Identification of missing prices.

d. Flagging of price variances beyond pre-established tolerance levels.

2.9.3.2 Recommendatory Elements

i. To enhance protection over outsourcing risk, AMCs may include the following as part of their evaluation / monitoring program:

a. Consider fraud vulnerabilities in the outsourced process, including:
   1. Detailed periodic fraud risk assessment program
   2. Fraud response plan
   3. Fraud risk register
   4. Reporting to the AMC's Board

b. Maintain an exit strategy including a pool of comparable service providers, in the event that a contracted service provider is unable to perform or in the event of a critical fraud.

2.10 Sales and Distribution Risk

2.10.1 As most AMCs outsource or use other channels for distributing products, such as banks, IAs, brokers, NBFCs, Distributors, etc., there is a need of monitoring risks associated with managing distribution channels and processes, commission pay-outs, brokerage disbursements, sales expenses, etc.

2.10.2 The mandatory and recommendatory elements for managing sales and distribution risk, are outlined below:

2.10.2.1 Mandatory Elements

i. The KRA/performance appraisal at the relevant CXO level must capture the performance in managing the risk of mis-selling. The risk of mis-selling may incorporate the components like the number of mis-sellings, outcomes in the inspection report, analysis

of the portfolio of investors, analysis based on assessment of appropriateness to the investors, etc. As an example, a parameter to gauge mis-selling may be the analysis of whether growth in the AUM of a scheme is on account of performance or mainly due to higher commission paid to distributor.

ii. The AMC shall also be responsible for the mis-selling done by the persons associated with selling of mutual funds including distributors. The performance disclosure to investors, if any, by the distributors should be true and fair. It should not be misleading to the investor by representing any selective time period representing the favorable return.

iii. Detailed analysis should be done at the AMC level to verify mis-sellings, if any.

iv. All the sales staff and distributers must be NISM certified with the required qualifications prescribed by SEBI/AMFI.

v. The AMC must implement the following procedures relating to distributor commissions:

    a. Analytical tools/ audit procedures used to review trends/errors in brokerage/ commission disbursements.
    b. An approved methodology for determining commission structures applicable to distributors / products, together with an authorization matrix for approving deviations and reporting cost-benefit outcome.
    c. Ensuring that commissions and other payments made to distributors adhere to AMFI and regulatory requirements.

vi. Conducting regular performance reviews for distributors.

vii. Conducting enhanced due diligence of distributors where appropriate (suitable policy to be incorporated)

2.10.2.2 Recommendatory Elements

i. Distribution risks can be further monitored by:

a. Monitoring marketing, sales and promotional expenses which includes the nature of expenses and approval matrix for the expenses.
b. Monitoring and reporting the cost-benefit outcome of the marketing, marketing, sales and promotional expenses
c. Undertaking mystery shopping.
d. Claw back provisions in the commission structures to provide adequate protection from continuous services to the investors.

2.11 Financial Reporting Risk

2.11.1 Absence of internal control over financial reporting with regard to the mutual fund schemes, may pose the following risks:

i. Improper maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of assets
ii. Absence of reasonable assurance that transactions are recorded as necessary to permit calculation of NAV and preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures are being made only in accordance with authorizations of the management and the Board
iii. Failure to prevent or timely detect unauthorized acquisition, use, or disposition of assets that could have a material effect on the NAV and/or financial statements.

2.11.2 The mandatory elements for managing financial reporting risk, are outlined below:

2.11.2.1 Mandatory Elements

i. The AMC should have detailed accounting policies and procedures for Mutual Fund accounting.
ii. Adequate segregation of duties must be created within the Finance (or relevant) function for Mutual Fund accounting.
iii. There should be documentation and regular testing of internal controls over financial reporting of Mutual Fund schemes.

2.12 Legal & Tax Risks

2.12.1 Legal & Tax risk is the risk of loss to an institution which is primarily caused by:

i. A defective transaction.
ii. A claim (including a defense to a claim or a counterclaim) being made or some other event occurring which results in a liability for the institution or other loss (for example, as a result of the termination of a contract).
iii. Failing to take appropriate measures to protect assets (for example, intellectual property) owned by the institution.
iv. Change in law
v. Misinterpretation of statutes and regulations.
vi. Failure to collect or pay appropriate taxes, or submit required returns or information.

2.12.2 The mandatory elements for managing legal and tax risk, are outlined below:

2.12.2.1 Mandatory Elements

i. The AMC should have documented processes and defined responsibilities for:
   a. Calculation and deposit statutory levies applicable to Mutual Funds.
   b. Acceptance of applications from permitted jurisdictions.
   c. Monitoring of risks emanating from tax related aspects and their redressal.
   d. Implementation of new and amended statutory and regulatory requirements.

ii. To mitigate legal risks, the AMC should have documented processes and defined responsibilities for:
   a. Review of material agreements.
   b. Authorized personnel for execution and registration of legal agreements and documents.
   c. Centralized register of all legal agreements
   d. Archival of physical and electronic versions of all legal agreements and documents.

2.13 Talent Risk

2.13.1 Talent risk is the risk of not having the right people in place at the right time to drive current and future business growth.

2.13.2 The mandatory and recommendatory elements for managing talent risk, are outlined below:

2.13.2.1 Mandatory Elements

i. With respect to talent risk, there should be proper succession planning for identified key positions. At no point of time the AMC is deprived of the services of any Key Managerial Person.

ii. The AMC should have adequately documented policies and procedures for:

   a. Recruiting staff with appropriate experience, skill levels, and degree of expertise to undertake specialized business operations., in particular, those relating to risk management
   b. Employing screening procedures, including background checks, for job applicants, particularly for key positions.
   c. Creation of policies for recruiting, retaining and remunerating staff, especially for key personnel.
   d. Evaluation of the candidate's capability and experience to manage the risks associated with the concerned role is should be a key element of the recruitment process.
   e. Adequate back-ups for key people are present.

2.13.2.2 Recommendatory Elements

i. AMCs may implement a remuneration policy that prevents excessive risk taking and also ensures retention of good talent.

ii. A Remuneration Committee, comprising mainly of non-executive directors may be established to review and recommend the policy relating to the remuneration of key management personnel, including the CEO, Fund Managers, etc.

ANNEXURE 2: INVESTMENT VALUATION NORMS FOR MUTUAL FUNDS[2]

All mutual funds shall provide transaction details of various types of debt securities like NCDs, Mibor linked floaters and CPs on daily basis in the format below to the agency recommended by AMFI. Submission of data would help in daily matrix generation, would improve uniformity and accuracy of valuation in the mutual funds industry.

Date Of Transaction	Coupon	Security Name	Security Type	Staggered Redemption/Maturity Dates	Staggered Redemption /Maturity Values	Rating	Put/Call Option Dates	Put/Call Option Values	Interest Payment Dates	Volume (in Rs. Crs)	Clean Price	YTM (Annualised)
			NCD									
			Mibor Linked									
			CP									

[2] SEBI Cir No - MFD/CIR.No 23 / 066 /2003 dated March 7, 2003

ANNEXURE 3: LIST OF MILLION PLUS CITIES

List of Million Plus Cities for investments by REMF[3]

Census of India 2001 (Provisional)

S.No.	Name of City	Civic Status	State/Union Territory
1	2	3	4
1	Greater Mumbai	M.Corp.	Maharashtra
2	Delhi Municipal Corporation (Urban)	M.Corp.	Delhi
3	Kolkata	M.Corp.	West Bengal
4	Bangalore	M.Corp.	Karnataka
5	Chennai	M.Corp.	Tamil Nadu
6	Ahmedabad	M.Corp.	Gujarat
7	Hyderabad	M.Corp.	Andhra Pradesh
8	Pune	M.Corp.	Maharashtra
9	Kanpur	M.Corp.	Uttar Pradesh
10	Surat	M.Corp.	Gujarat
11	Jaipur	M.Corp	Rajasthan
12	Lucknow	M.Corp.	Uttar Pradesh
13	Nagpur	M.Corp.	Maharashtra
14	Indore	M.Corp.	Madhya Pradesh
15	Bhopal	M.Corp.	Madhya Pradesh
16	Ludhiana	M.Corp.	Punjab
17	Patna	M.Corp	Bihar
18	Vadodara	M.Corp.	Gujarat
19	Thane	M.Corp.	Maharashtra
20	Agra	M.Corp.	Uttar Pradesh
21	Kalyan-Dombivli	M.Corp.	Maharashtra
22	Varanasi	M.Corp.	Uttar Pradesh
23	Nashik	M.Corp.	Maharashtra
24	Meerut	M.Corp.	Uttar Pradesh
25	Faridabad	M.Corp.	Haryana
26	Haora	M.Corp.	West Bengal
27	Pimprichinchwad	M.Corp.	Maharashtra

[3] SEBI/IMD/CIR No.4/124477/08 dated May 2, 2008

Total:

Note:

M. Corp. stands for Municipal Corporation

List of Million Plus UAs Cities for investments by REMF

Urban Agglomerations/Cities having population of more than one million in 2001

Rank in 2001	Urban Agglomeration/City (1,000,000 + population)	Civic Status
1	2	3
1	Greater Mumbai	UA
2	Kolkata	UA
3	Delhi	UA
4	Chennai	UA
5	Bangalore	UA
6	Hyderabad	UA
7	Ahmadabad	UA
8	Pune	UA
9	Surat	UA
10	Kanpur	UA
11	Jaipur	M.Corp.
12	Lucknow	UA
13	Nagpur	UA
14	Patna	UA
15	Indore	UA
16	Vadodara	UA
17	Bhopal	UA
18	Coimbatore	UA
19	Ludhiana	M.Corp.
20	Kochi	UA
21	Visakhapatnam	UA
22	Agra	UA
23	Varanasi	UA
24	Madurai	UA
25	Meerut	UA
26	Nashik	UA
27	Jabalpur	UA
28	Jamshedpur	UA
29	Asansol	UA
30	Dhanbad	UA
31	Faridabad	M.Corp.

32	Allahabad	UA
33	Amritsar	UA
34	Vijayawada	UA
35	Rajkot	UA
	TOTAL	

ANNEXURE 4: FREQUENTLY ASKED QUESTIONS (FAQs)

1. SEBI has prepared a FAQs on mutual funds. The same is updated by SEBI from time to time. FAQs are available on SEBI website under "SEBI Website -> FAQs -> Mutual Funds".

2. Link for accessing FAQs is given below:

Details	**Link**
FAQs for Mutual Fund Intermediaries	https://www.sebi.gov.in/sebi_data/faqfiles/apr-2023/1682683461615.pdf
FAQs for Mutual Fund Investors	https://www.sebi.gov.in/sebi_data/faqfiles/apr-2023/1682683491126.pdf

ANNEXURE 5: GAZETTE NOTIFICATION DATED MAY 31, 2010[4]

THE GAZETTE OF INDIA

EXTRAORDINARY

PART - III - SECTION 4

PUBLISHED BY AUTHORITY

NEW DELHI, MAY 31, 2010

SECURITIES AND EXCHANGE BOARD OF INDIA

NOTIFICATION

Mumbai, the 31st May, 2010

Notification under regulation 3 of the Securities and Exchange Board of India (Certification of Associated Persons in the Securities Markets) Regulations, 2007.

In terms of sub-regulation (1) of regulation 3 of the Securities and Exchange Board of India (Certification of Associated Persons in the Securities Markets) Regulations, 2007 (the Regulations), the Board is empowered to require, by notification, any category of associated persons as defined in the Regulations to obtain requisite certification.

Accordingly, it is notified that with effect from June 01, 2010, the following category of associated persons, i.e., distributors, agents or any persons employed or engaged or to be employed or engaged in the sale and/or distribution of mutual fund products, shall be required to have a valid certification from the National Institute of Securities Markets (NISM) by passing the certification examination as mentioned in the NISM communiqué NISM/Certification/Series-V-A: MFD/2010/01 dated May 05, 2010.

[4] SEBI Cir no Cir / IMD / DF / 5 / 2010 dated June 24, 2010

Provided that if the said associated person possesses a valid certificate by passing before June 01, 2010, the AMFI Mutual Fund (Advisors) Module, he shall be exempted from the requirement of the aforementioned NISM certification examination.

LAD-NRO/GN/2010-11/09/6422

C. B. BHAVE
CHAIRMAN
SECURITIES AND EXCHANGE BOARD OF INDIA

ANNEXURE 6: CYBER SECURITY AND CYBER RESILIENCE FRAMEWORK FOR MUTUAL FUNDS/ ASSET MANAGEMENT COMPANIES (AMCs)[5]

1. Cyber-attacks and threats attempt to compromise the Confidentiality, Integrity and Availability (CIA) of the computer systems, networks and databases (Confidentiality refers to limiting access of systems and information to authorized users, Integrity is the assurance that the information is reliable and accurate, and Availability refers to guarantee of reliable access to the systems and information by authorized users). Cyber security framework includes measures, tools and processes that are intended to prevent cyber-attacks and improve cyber resilience. Cyber Resilience is an organization's ability to prepare and respond to a cyber-attack and to continue operation during, and recover from, a cyber-attack.

Governance

2. As part of the operational risk management framework to manage risk to systems, networks and databases from cyber-attacks and threats, Mutual Funds/ Asset Management Companies (AMCs) should formulate a comprehensive cyber security and cyber resilience policy document encompassing the framework mentioned hereunder. The policy document should be approved by the Board of the AMC and Trustees, and in case of deviations from the suggested framework, reasons for such deviations should also be provided in the policy document. The policy document should be reviewed by the Board of AMC at least once annually with the view to strengthen and improve its cyber security and cyber resilience framework.

[5] SEBI Cir No SEBI/HO/IMD/DF2/CIR/P/2019/12 dated January 10, 2019 & SEBI Circular No. SEBI/HO/IMD/IMD-I/DOF2/P/CIR/2022/81 dated June 9, 2022

3. The cyber security and cyber resilience policy should include the following process to identify, assess, and manage cyber security risk associated with processes, information, networks and systems;

    a. 'Identify' critical IT assets and risks associated with such assets,
    b. 'Protect' assets by deploying suitable controls, tools and measures,
    c. 'Detect' incidents, anomalies and attacks through appropriate monitoring tools/processes,
    d. 'Respond' by taking immediate steps after identification of the incident, anomaly or attack,
    e. 'Recover' from incident through incident management, disaster recovery and business continuity framework.

4. The Cyber security policy should encompass the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organization (NTRO), Government of India, in the report titled 'Guidelines for Protection of National Critical Information Infrastructure' and subsequent revisions, if any, from time to time.

5. Mutual Funds/ AMCs should also incorporate best practices from standards such as ISO 27001, ISO 27002, COBIT 5, etc., or their subsequent revisions, if any, from time to time.

6. Mutual Funds/ AMCs should designate a senior official as Chief Information Security Officer (CISO) whose function would be to

assess, identify and reduce cyber security risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the cyber security and resilience policy approved by the Board of the AMCs.

7. The Board of the AMCs shall constitute a Technology Committee comprising experts proficient in technology. This Technology Committee should on a quarterly basis review the implementation of the cyber security and cyber resilience policy approved by their Board, and such review should include review of their current IT and cyber security and cyber resilience capabilities, set goals for a target level of cyber resilience, and establish a plan to improve and strengthen cyber security and cyber resilience. The review shall be placed before the Board of the AMCs and Trustees for appropriate action.

8. Mutual Funds/ AMCs should establish a reporting procedure to facilitate communication of unusual activities and events to CISO or to the senior management in a timely manner.

9. The aforementioned committee and the senior management of the AMCs, including the CISO, should periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen cyber security and cyber resilience framework.

10. Mutual Funds/ AMCs should define responsibilities of its employees, outsourced staff, and employees of vendors, members or participants and other entities, who may have access or use systems / networks of the Mutual Funds/ AMCs, towards ensuring the goal of cyber security.

Identify

11. Mutual Funds/ AMCs shall identify and classify critical assets based on their sensitivity and criticality for business operations, services and data management. The critical assets shall include business critical systems, internet facing applications/ systems, systems that contain sensitive data, sensitive personal data, sensitive financial data, Personally Identifiable Information (PII) data, etc. All the ancillary systems used for accessing/ communicating with critical systems either for operations or maintenance shall also be classified as critical assets. The Board of the AMCs and Trustees shall approve the list of critical assets.

    To this end, Mutual Funds/ AMCs shall maintain up-to-date inventory of its hardware and systems, software and information assets (internal and external), details of its network resources, connections to its network and data flows..

12. Mutual Funds/ AMCs should accordingly identify cyber risks (threats and vulnerabilities) that it may face, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.

13. Mutual Funds/ AMCs should also encourage its third-party service providers, if any, such as RTAs, Custodians, Brokers, Distributors, etc. to have similar standards of Information Security.

Protection

Access Controls

14. No person by virtue of rank or position should have any intrinsic right to access confidential data, applications, system resources or facilities.

15. Any access to AMC's/ Mutual Fund's systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period. AMCs/MFs should grant access to IT systems, applications, databases and networks on a need-to-use basis and based on the principle of least privilege. Such access should be for the period when the access is required and should be authorized using strong authentication mechanisms.

16. Mutual Funds/ AMCs should implement strong password controls for users' access to systems, applications, networks and databases. Password controls should include a change of password upon first log-on, minimum password length and history, password complexity as well as maximum validity period. The user credential data should be stored using strong and latest hashing algorithms.

17. Mutual Funds/ AMCs should ensure that records of user access are uniquely identified and logged for audit and review purposes. Such logs should be maintained and stored in encrypted form for a time period not less than two (2) years.

18. Mutual Funds/ AMCs should deploy additional controls and security measures to supervise staff with elevated system access

entitlements (such as admin or privileged users). Such controls and measures should inter-alia include restricting the number of privileged users, periodic review of privileged users' activities, disallow privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.

19. Account access lock policies after failure attempts should be implemented for all accounts.

20. Employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to the Mutual Fund's/ AMC's critical systems, networks and other computer resources, should be subject to stringent supervision, monitoring and access restrictions.

21. Two-factor authentication at log-in should be implemented for all users that connect using online/ internet facility.

22. Mutual Funds/ AMCs should formulate an Internet access policy to monitor and regulate the use of internet and internet based services such as social media sites, cloud-based internet storage sites, etc.

23. Proper 'end of life' mechanism should be adopted to deactivate access privileges of users who are leaving the organization or whose access privileges have been withdrawn.

Physical Security

24. Physical access to the critical systems should be restricted to minimum. Physical access of outsourced staff or visitors should be properly supervised by ensuring at the minimum that outsourced staff or visitors are accompanied at all times by authorized employees.

25. Physical access to the critical systems should be revoked immediately if the same is no longer required.

26. Mutual Funds/ AMCs should ensure that the perimeter of the critical equipments rooms are physically secured and monitored by employing physical, human and procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. where appropriate.

Network Security Management

27. Mutual Funds/ AMCs should establish baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within the IT environment. The Mutual Funds/ AMCs should conduct regular enforcement checks to ensure that the baseline standards are applied uniformly.

28. Mutual Funds/ AMCs should install network security devices, such as firewalls as well as intrusion detection and prevention systems, to protect their IT infrastructure from security exposures originating from internal and external sources.

29. Anti-virus software should be installed on servers and other computer systems. Updation of anti-virus definition files and automatic anti-virus scanning should be done on a regular basis.

Security of Data

30. Data-in motion and Data-at-rest should be in encrypted form by using strong encryption methods such as Advanced Encryption Standard (AES), RSA, SHA-2, etc.

31. Mutual Funds/ AMCs should implement measures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity. It should be ensured that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties.

32. The information security policy should also cover use of devices such as mobile phone, faxes, photocopiers, scanners, etc. that can be used for capturing and transmission of data.

33. Mutual Funds/ AMCs should allow only authorized data storage devices through appropriate validation processes.

Hardening of Hardware and Software

34. Only a hardened and vetted hardware / software should be deployed by the Mutual Funds/ AMCs. During the hardening process, Mutual Funds/ AMCs should inter-alia ensure that default passwords are replaced with strong passwords and all

unnecessary services are removed or disabled in equipments / software.

35. All open ports which are not in use or can potentially be used for exploitation of data should be blocked. Other open ports should be monitored and appropriate measures should be taken to secure the ports.

Application Security and Testing

36. Mutual Funds/ AMCs should ensure that regression testing is undertaken before new or modified system is implemented. The scope of tests should cover business logic, security controls and system performance under various stress-load scenarios and recovery conditions.

Patch Management

37. Mutual Funds/ AMCs should establish and ensure that the patch management procedures include the identification, categorization and prioritization of security patches. An implementation timeframe for each category of security patches should be established to implement security patches in a timely manner.

38. Mutual Funds/ AMCs should perform rigorous testing of security patches before deployment into the production environment so as to ensure that the application of patches do not impact other systems.

Disposal of systems and storage devices

39. Mutual Funds/ AMCs should frame suitable policy for disposals of the storage media and systems. The data / information on such devices and systems should be removed by using methods viz. wiping / cleaning / overwrite, degauss and physical destruction, as applicable.

Vulnerability Assessment and Penetration Testing (VAPT)

40. Mutual Funds/ AMCs shall carry out periodic VAPT, inter-alia, including critical assets and infrastructure components like servers, networking systems, security devices, load balancers, other IT systems pertaining to the activities done as a role of Mutual Funds/ AMCs, etc., in order to detect security vulnerabilities in the IT environment and in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks. Mutual Funds/ AMCs shall conduct VAPT at least once in a financial year. However, for the Mutual Funds/ AMCs, whose systems have been identified as "protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC) under the Information Technology (IT) Act, 2000, VAPT shall be conducted at least twice in a financial year. Further, all Mutual Funds/ AMCs shall engage only Indian Computer Emergency Response Team (CERT-In) empanelled organizations for conducting VAPT. The final report on said VAPT shall be submitted to SEBI after approval from Technology Committee of respective Mutual Funds/ AMCs, within 1 month of completion of VAPT activity.

41. Any gaps or vulnerabilities detected shall be remedied on immediate basis and compliance of closure of findings identified during VAPT shall be submitted to SEBI within 3 months post the submission of final VAPT report.

42. In addition, Mutual Funds/ AMCs shall perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system which is a critical system or part of an existing critical system.

Monitoring and Detection

43. Mutual Funds/ AMCs should establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events and timely detection of unauthorized or malicious activities, unauthorized changes, unauthorized access and unauthorized copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices should also be monitored for anomalies.

44. Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks, Mutual Funds/ AMCs should implement suitable mechanism to monitor capacity utilization of its critical systems and networks.

45. Suitable alerts should be generated in the event of detection of unauthorized or abnormal system activities, transmission errors or unusual online transactions.

Response and Recovery

46. Alerts generated from monitoring and detection systems should be suitably investigated, including impact and forensic analysis of such alerts, in order to determine activities that are to be performed to prevent expansion of such incident of cyber-attack or breach, mitigate its effect and eradicate the incident.

47. The response and recovery plan of the Mutual Funds/ AMCs should aim at timely restoration of systems affected by incidents of cyber-attacks or breaches. The recovery plan should be in line with the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as specified by SEBI for Market Infrastructure Institutions vide SEBI circular CIR/MRD/DMS/17/20 dated June 22, 2012 as amended from time to time.

48. The response plan should define responsibilities and actions to be performed by its employees and support or outsourced staff in the event of cyber-attacks or breach of cyber security mechanism.

49. Any incident of loss or destruction of data or systems should be thoroughly analyzed and lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes.

50. Mutual Funds/ AMCs should also conduct suitable periodic drills to test the adequacy and effectiveness of response and recovery plan.

Sharing of information

51. All cyber-attacks, threats, cyber-incidents, and breaches experienced by Mutual Funds/ AMCs shall be reported to SEBI within 6 hours of noticing/ detecting such incidents or being brought to their notice about such incidents. The incident shall also be reported to CERT-In in accordance with the guidelines/ directions issued by CERT-In from time to time. Additionally, the Mutual Funds/ AMCs, whose systems have been identified as "protected system" by NCIIPC, shall also report the incident to NCIIPC. The quarterly reports containing information on cyber-attacks, threats, cyber-incidents, and breaches experienced by Mutual Funds/ AMCs and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs/ vulnerabilities/ threats that may be useful for other Mutual Funds/ AMCs shall be submitted to SEBI within 15 days from the quarter ended June, September, December and March of every year.

52. Such details as are felt useful for sharing with other Mutual Funds/ AMCs in masked and anonymous manner shall be shared using mechanism to be specified by SEBI from time to time.

Training

53. Mutual Funds/ AMCs should conduct periodic training programs to enhance awareness level among the employees and outsourced staff, vendors, etc. on IT / Cyber security policy and standards. Special focus should be given to build awareness levels and skills of staff from non-technical disciplines.

54. The training program should be reviewed and updated to ensure that the contents of the program remain current and relevant.

Periodic Audit

55. AMCs / Mutual Funds shall arrange to have its systems audited on an semi-annual basis by an independent CISA / CISM qualified or CERT-IN empanelled auditor to check compliance with the above areas and shall submit the report to SEBI along with the comments of the Board of AMCs and Trustees within three months of the end of the financial year.

Vendors or Service Providers

56. AMCs / MFs have outsourced many of their critical activities to different agencies / vendors / service providers. The responsibility, accountability and ownership of those outsourced activities lies primarily with AMCs / MFs. Therefore, AMCs / MFs have to come out with appropriate monitoring mechanism through clearly defined framework to ensure that all the requirements as specified in this Annexure are complied with. The periodic report submitted to SEBI should highlight the critical activities handled by the agencies and to certify the above requirement is complied. The provisions of this Annexure shall also apply to those RTAs which serves AMCs as the in-house RTAs of the AMCs.

ANNEXURE 7: REPORTING FOR ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML) APPLICATIONS AND SYSTEMS OFFERED AND USED BY MUTUAL FUNDS[6]

Systems deemed to be based on AI and ML technology

Applications and Systems belonging but not limited to following categories or a combination of these:

1. Natural Language Processing (NLP), sentiment analysis or text mining systems that gather intelligence from unstructured data. – In this case, Voice to text, text to intelligence systems in any natural language will be considered in scope. E.g.: robo chat bots, big data intelligence gathering systems.

2. Neural Networks or a modified form of it. – In this case, any systems that uses a number of nodes (physical or software simulated nodes) mimicking natural neural networks of any scale, so as to carry out learning from previous firing of the nodes will be considered in scope. E.g.: Recurrent Neural networks and Deep learning Neural Networks.

3. Machine learning through supervised, unsupervised learning or a combination of both. – In this case, any application or systems that carry out knowledge representation to form a knowledge base of domain, by learning and creating its outputs with real world input data and deciding future outputs based upon the knowledge base. E.g.: System based on Decision tree, random forest, K mean, Markov decision process, Gradient boosting Algorithms.

[6] SEBI Cir No SEBI/HO/IMD/DF5/CIR/P/2019/63 dated May 09, 2019

4. A system that uses statistical heuristics method instead of procedural algorithms or the system / application applies clustering or categorization algorithms to categorize data without a predefined set of categories.

5. A system that uses a feedback mechanism to improve its parameters and bases it subsequent execution steps on these parameters.

6. A system that does knowledge representation and maintains a knowledge base.

ANNEXURE 8: SYSTEM AUDIT[7]

System Audit framework for Mutual Funds/ Asset Management Companies (AMCs)

IT Environment				
Organization Details				
Name				
Address				
What is the IT team size (Employees)?				
What is the IT team size (Vendors)?				
IT Setup & Usage				
Data Center and DR Site (Location, owned/outsourced)				
Network Diagram (schematic) with WAN connectivity				
Network/ Security Systems: (Please specify Version/make/model)				
- Routers				
- Switches				
- Proxy servers				
- Firewall				
- Intrusion Detection Systems				
- Intrusion Prevention Systems				
- Remote Access Servers				
- Data Leakage Prevention (specify network and/ or host)				
- Privileged Identity Management				
- Others (please specify e.g. WIPS)				
Total number of workstations (incl. laptops) & users				
Primary Operating Systems in use for workstations?				
Application Systems				
Application System	**Location of server(s)**	**HW/OS/DB for DB Server**	**HW/OS/DB for Web Server**	**HW/OS/DB for Web Server**
e.g. Front Office System				
e.g. Back Office System				
e.g. Email System				

[7] SEBI Circular No. SEBI/HO/IMD/DF2/CIR/P/2019/57 dated April 11, 2019

e.g. Intranet System				
e.g. File Server System				
e.g. Finance & Accounting System				

System Audit Program Checklist

The checklist is intended to provide guidance to the Mutual Funds/Asset Management (MFs/AMCs) Companies and Firms/ Companies appointed by MFs/AMCs for performing the systems audit. MFs/AMCs are responsible for ensuring that adequate and effective control environment exists over the IT systems in use for supporting business operations, including that at vendors/ third parties supporting operations like Register & Transfer Agents (RTAs), Fund Accountants, Custodians etc.

Audit Objective Question No	Audit Objective Heading	Sub-Heading	Audit Checklist
1	**IT GOVERNANCE**		**IT GOVERNANCE**
1a	**IT GOVERNANCE**	**IT Governance Framework**	**IT Governance framework:** Whether an IT Governance framework exists which requires defining of: - An IT Organization Structure - Frameworks used for IT governance - Organization wide IT governance processes including policy making, implementation and monitoring to ensure that the governance principles are followed as desired
1b	**IT GOVERNANCE**	**IT Strategy Committee**	**IT Strategy Committee:** - Whether an IT Strategy Committee exists with representations from Board of Directors (BOD), senior IT and business management and reporting to the BOD? - Is the IT strategy committee has members with skills and understanding of processes, information technology and information security in the context of Mutual Fund and other business of the organization? - Are roles and responsibilities of the IT Strategy Committee defined? - Does the IT Strategy Committee meet at least twice in a year?
1c	**IT GOVERNANCE**	**IT Risk Management**	**IT Risk Management:** - Whether organization has a defined IT risk management framework covering amongst others process and responsibilities of risk assessment, management and monitoring? - Does the risk management framework include the following: a. Identification of IT assets subject to risk management b. Identification of threats related to those IT assets c. Assessment of probability of occurrence of threats d. Defining risk mitigation methods in line with threats, risk categorization and probability e. Process to be followed for monitoring of risks identified and mitigation methods implemented - Is the IT risk management framework approved by the BOD?

			- Has the organization established risk management committee that oversee and provide direction with respect to IT risk?
1d	**IT GOVERNANCE**	**IT Policies and Procedures:**	**IT Policies and Procedures:** - Whether a defined and documented IT policy exists and is approved by the BOD? - Is the current state of IT architecture documented including infrastructure, network and application components to show system linkages and dependencies? - Whether defined and documented procedures exist for all components, which amongst others include: a. IT Assets Acquisition (including retrial) b. Logical access management c. Change management d. Backup and recovery e. Automated batch jobs f. Incident management g. Problem management h. Data Center Operations i. Operating systems and database management j. Network and communication management k. End user computing l. Acceptable use of IT assets, etc. - Does IT policy comprise of the IT organization structure, roles and responsibilities of key IT management personnel, IT strategic management process and processes for ensuring adherence with compliance requirements?
1e	**IT GOVERNANCE**	**IT Organization Structure**	**IT Organization Structure:** - Whether a defined organization structure exists with defined authorities, reporting lines and responsibilities related to IT governance including a designated Chief Information Officer (CIO)/ Chief Technology Officer (CTO), Chief Information Security Officer (CISO) and heads for key IT teams managing IT operations, IT applications, IT infrastructure, IT risk management/ reviews? - Are roles and responsibilities of IT Organization defined?
1f	**IT GOVERNANCE**	**IS Audit**	**Information Systems (IS) Audit:** - Is there a defined IS audit framework including process and responsibilities to be followed for IS audits, IS audit calendar, scope definition, review, reporting process and monitoring progress against non-compliances? - Are IS audit plans, reports, findings and action plans reported management and audit committee of board as appropriate?
2	**INFORMATION SECURITY**		**INFORMATION SECURITY**
2a	**INFORMATION SECURITY**	**Information Security function**	**Information Security function:** - Whether an information security function exists distinct from IT function with dedicated responsibility of defining and monitoring implementation of information security policies and controls? - Is there a designated CISO responsible for overseeing

			the information security function and for ensuring information security procedures are defined and implemented? - Does the information security function include representations from departments and operations across the organization including internal and client facing functions and including all organization locations?
2b	**INFORMATION SECURITY**	**Information Security policy**	**Information Security policy:** - Whether a defined and documented information security policy exists and is approved by the BOD? - Whether the information security framework ensures security requirements are in-built into key IT architecture, operations and other non-IT aspects, including but not limited to: a. Access management - Physical and Logical b. Infrastructure and applications change management c. Backup and recovery d. automated batch jobs e. Incident management (including security incidents) f. Problem management g. Data center Operations h. Operating systems and database management i. Network and communication management j. End user computing, in addition consider phone, faxes, photocopiers, scanners, etc. k. Security Operations - logging and monitoring - Whether defined and documented procedures exist for the following: a. Hardening procedures, standards and guidelines for operating systems, databases, servers and network devices b. Use of cryptography c. Third Party Security d. Human Resource controls for information security e. Information classification guidance and process including mechanisms for storage, transmission and disposal of information - Whether the information security framework/ policy is reviewed on an yearly basis at a minimum?
2c	**INFORMATION SECURITY**	**Information Security Risk Management**	**Information Security Risk Management:** - Whether a defined process exists and is followed for Information Security (IS) risk management on an annual basis, at a minimum? - Whether the IS risk management is performed in line with the organization and IT risk management framework? - Whether the risk assessment is performed for new functions, processes, teams and locations. Whether relevant risk mitigation and monitoring actions are implemented as per the defined framework?
2d	**INFORMATION SECURITY**	**Cyber Security**	**Cyber Security:** - Whether Mutual Funds / AMCs has complied with the provisions of Cyber Security and Cyber Resilience prescribed under Paragraph 4.7 of the Master Circular and any further guidelines by SEBI with regard to cyber security for MFs / AMCs?

2e	**INFORMATION SECURITY**	**Information Security Awareness**	**Information Security Awareness:** - Whether information security and cybersecurity processes are communicated to employees, contractors, third parties, etc.? - Whether information security and cybersecurity trainings are conducted as part of induction as well as periodic trainings?
2f	**INFORMATION SECURITY**	**Information Privacy**	**Information Privacy:** - Whether defined and documented privacy policy exists and is approved by the BOD? - Whether procedures have been defined in line with applicable regulations with respect to: a. Privacy notice b. Choice & consent c. Data collection d. Data use, retention & disposal e. Access to data f. Disclosure to third parties g. Security controls for private data h. Monitoring & enforcement
2g	**INFORMATION SECURITY**	**Human Resource Controls**	**Human Resource Controls:** - Whether policies and procedures have been implemented to address HR controls as part of information security? - Whether hiring policies are defined in line with IT operations and information security requirements? - Whether induction trainings are conducted for all new joiners? - Whether all new joiners are required to confirm and accept the organization's policies and procedures with respect to information technology, information security and cybersecurity? - Whether background check procedures are performed for all new joiners?
2h	**INFORMATION SECURITY**	**Digital Technologies**	**Digital Technologies:** - Whether the organization has a defined process to identify, develop and implement digital technologies supporting internal and external facing functions? - Whether all digital technologies including mobile applications, web-based portals, mobile websites, cloud storage, etc. are implemented only after performing risk assessment, testing and where required independent reviews? - Whether the organization has a defined and approved social media usage policy to address information security and reputational risks arising out of the same?
2i	**INFORMATION SECURITY**	**Third Party Security**	**Third Party Security:** - Whether the organization has a defined vendor management framework and is approved by the BOD? - Whether the vendor management framework includes processes to be followed for vendor due diligence, selection, risk assessment, onboarding, contracting and monitoring? - Whether vendors are on boarded only after performing a technical due diligence, risk assessment

			and background checks? - Whether formal contracts are signed with vendors and include the following at a minimum: a. Services provided b. Processes to be followed c. Service Level Agreements and related penalty clauses, if any d. Confidentiality, service continuity and data privacy clauses e. Performance monitoring processes and reports to be provided f. Escalation procedures g. Right to access and audit
2j	**INFORMATION SECURITY**	**Information Security Compliance**	**Information Security Compliance:** - Has the organization implemented procedures to assess compliance against defined information security procedures in the form of periodic assessments/ reviews? - Are critical functions within the organization subject to stringent security reviews by internal teams or external agencies, where necessary? - Are IS review reports, findings and action plans reported to IT/IS risk committees, IT Strategy Committee of BOD as appropriate?
3	**ACCESS MANAGEMENT**		**ACCESS MANAGEMENT**
3a	**ACCESS MANAGEMENT**	**Access Policies and procedures**	**Access Policies and procedures:** - Whether defined and documented policies and procedures exist for managing access to applications and infrastructure (including network, operating systems and database) and are approved by relevant authority? - Whether the defined procedures include responsibilities and process to be followed for: a. Access grant and modification including definition of authorization matrix as per system b. Access revocation procedures including notification as well as timeliness of revocation c. Access rights and Roles review procedures for all systems d. Privileged access to systems e. Review of access logs for privileged users f. Segregation of Duties (SOD) - Whether appropriate risk acceptance is taken 0in the event entire approved procedures ca0nnot be implemented due to system limitations? In such cases, whether alternate risk mitigation measures are implemented?
3b	**ACCESS MANAGEMENT**	**Privileged access**	**Privileged access:** - Whether privileged access to systems is available to limited authorized personnel? - Whether privileged access to systems is subject to more stringent security controls (such as Privileged Identity Management Solutions, more stringent password parameters, etc.) as compared to normal users? - Whether access rights for privileged users are monitored on periodic basis?

			- Whether logs of privileged users are stored and reviewed on a periodic basis based on criticality of systems?
3c	**ACCESS MANAGEMENT**	**Access Administration**	**Access Administration:** - Whether role-based and least privilege access mechanisms are in-built into systems to enable authorized access as per job roles? - Whether access administration requests, related approvals/ notifications and related actions (creations, revocation and modification) are logged and documented using automated tools with date-time stamps and appropriate evidences are retained as per defined procedures for review and audit purpose? - Whether creation and modification of access to systems requires a formal approval based on a defined authorization matrix? - Whether access revocation notifications are sent on a timely basis? - Whether access is revoked on a timely basis on the last working date of the user? - Whether sufficient monitoring mechanisms have been implemented to ensure all access administration requests are addressed as per procedures? - Whether users are provided with unique user identifier as per organizations naming conventions?
3d	**ACCESS MANAGEMENT**	**Access Authentication**	**Access Authentication:** - Whether appropriate authentication mechanisms are used for access to systems including use of passwords, One Time Passwords (OTP), Single Sign on, etc.? - Following password parameters should be defined [In brackets some prevalent practices are shared]: a. Minimum length (e.g. 8 characters) b. Complexity (combination of alphabets (upper case and lower case)/ numbers/ symbols.) c. Maximum Age (e.g. 90 days) d. History (e.g. 3) e. Account lockout threshold (e.g. 3 or 5 attempts) - Whether defined procedures require usage of unique user IDs for each individual? - Whether usage of generic IDs and default IDs is prohibited unless necessary and with risk acceptance sign-off? In such cases ownership and accountability for usage of generic IDs should be documented. -Whether the system allows for automatic session logout after a system defined period of inactivity?
3e	**ACCESS MANAGEMENT**	**Access Review and Monitoring**	**Access Review and Monitoring:** - Whether access rights to systems are reviewed on a periodic basis based on criticality of systems? - Whether access logs of users having access to critical activities are monitored? - Whether rule based automated or manual alerts are implemented for unauthorized access or activities, whether such alerts are monitored and addressed on a timely basis? - Whether audit trails of critical activities including key business transactions, modification of security parameters, masters' updates, and access

			administration activities are available with details around related user IDs, approvers and date-time stamps. Whether audit trails are retained for evidence, review and audit purposes? - Whether control mechanisms such as periodic reconciliation of user lists with HR lists, deactivation of users with no logins for a defined timeframe, etc. have been deployed to ensure any unauthorized access is timely terminated?
3f	**ACCESS MANAGEMENT**	**Segregation of Duties (SOD)**	**Segregation of Duties (SOD):** - Whether a defined and documented SOD matrix exists describing key roles within the systems and conflicting rights? - Whether access approvals, creations and modifications are performed based on approved SOD matrix? - Potential SOD conflicts are investigated during periodic access reviews and corrective actions are taken, if any.
3g	**ACCESS MANAGEMENT**	**Physical Access Administration**	**Physical Access Administration:** - Whether defined and documented procedures exist for managing physical access to data center and processing facilities? - Whether creation of physical access requires documentation of appropriate approvals as per authorization matrix? - Whether revocation of physical access is performed on a timely basis on the last working day of the user? - Whether physical access administration requests, related approvals/ notifications and related actions (creations and modification) are logged and documented using automated tools with date-time stamps and appropriate evidences are retained as per defined procedures for review and audit purpose? - Whether access to restricted areas is reviewed at least once a year? - Whether physical access logs are available and retained for investigation purpose as per guidelines? - Whether physical access related incidents and invalid access attempts are monitored on a periodic basis?
3h	**ACCESS MANAGEMENT**	**Physical Security**	**Physical Security:** - Whether appropriate physical security mechanisms have been deployed including guarding entrance, usage of access control system, door alarms, turnstiles, biometric access, etc.? - Whether appropriate visitor access controls have been implemented including logging of visitor access including equipment carried, visitor escorting, issue and reconciliation of visitor badges, etc.? - Whether Closed Circuit Tele Vision (CCTV) has been installed in restricted areas for monitoring, and logs for the same are retained for investigation purpose? - Whether appropriate environmental security measures such as fire alarms, smoke detectors, water detectors, Air-conditioners, etc. have been implemented. Whether environmental controls are monitored on a periodic basis. Are environmental

			security devices maintained at regular intervals as prescribed by the vendor?
4	**CHANGE MANAGEMENT**		**CHANGE MANAGEMENT**
4a	**CHANGE MANAGEMENT**	**Change Management Policies and Procedures**	**Change Management Policies and Procedures:** - Whether organization has established formalized change management policy and procedures that define processes to be followed for changes made to all systems including applications and infrastructure (networks, operating systems, databases, etc.) including emergency and configuration changes, capturing the version history and approval history? - Whether appropriate guidance is available for categorization and prioritization of changes?
4b	**CHANGE MANAGEMENT**	**Change Administration**	**Change Administration:** - Whether changes to applications and infrastructure (networks, operating systems and databases), including requests to third party service providers are approved and authorized by both authorized IT and business management personnel, as per defined authorization matrix? - Whether for each change, a risk evaluation process is carried out and results of the same are approved by authorized personnel? -Whether test cases library is maintained and updated to enable comprehensive testing? - Whether changes for relevant applications, including infrastructure changes are tested and documented during User Acceptance testing (UAT). Whether there is a formal signoff of the UAT results provided by the business prior to implementation? - Whether changes for applications, including infrastructure (OS/DB) changes are tested and documented during system, unit, and regression testing, where applicable. Whether there is a formal signoff of the test results by the technology team prior to UAT performed by business? - Whether the procedures require sign-off from information security team for ensuring that security controls have been in-built into the systems? - Whether a post implementation review is performed and recorded for each change migrated to production environment? - Whether there exists a procedure to log emergency changes made to relevant applications and underlying infrastructure, which are authorized by business and IT management within defined time frame of being migrated to production environment? - Whether new systems or modules including major changes are subject to application security testing before deployment? - Whether software development is performed based on industry accepted coding standards?
4c	**CHANGE MANAGEMENT**	**Segregation of Duties (SOD), environments and version control**	**Segregation of Duties (SOD), environments and version control:** - Whether there exists a segregation of production, development and test environments? - Whether the organization has implemented a change

			management versioning tool to maintain audit trails for all types of changes including applications, databases, operating systems and networks? - Whether implemented changes are reviewed on a periodic basis and inappropriate or unauthorized activities are investigated and communicated to respective individuals? - Whether a formal process exists for granting user access to migrate changes to the production environment for relevant applications based upon approval by authorized personnel? - In case of any new system or module implementation, whether adequate procedures were performed to ensure accurate and complete transfer of data?
5	**INCIDENT MANAGEMENT**		**INCIDENT MANAGEMENT**
5a	**INCIDENT MANAGEMENT**	**Incident Management Policies and Procedures**	**Incident Management Policies and Procedures:** - Whether management has established formalized incident management policy and procedures that define processes to be followed for incidents related to all systems including applications and infrastructure (networks, operating systems, databases, etc.) capturing the version history and approval history? - Whether appropriate guidance is available for categorization and prioritization of incidents?
5b	**INCIDENT MANAGEMENT**	**Incident Resolution**	**Incident Resolution:** - Whether incidents are logged using automated tools with a unique ID assigned to each incident? - Whether incidents are classified based on their severity and urgency. Whether severity of incidents can be changed only by authorized personnel? - Whether a root cause analysis is performed for each incident and documented? - Whether a known error database is maintained for resolution and workaround details for similar incidents? - Whether details of resolution provided against each incident is documented against the ticket logged? - Whether incidents are tracked and monitored for resolution on a timely basis? - Whether recurring incidents are identified and logged as problems?
5c	**INCIDENT MANAGEMENT**	**Service Level Agreements (SLAs)**	**Service Level Agreements (SLAs):** - Whether formal SLAs have been defined for each incident type and agreed with business and the incident management team? - Whether SLAs are tracked using automated tools to identify timely escalation to be performed? - Whether escalation matrix has been defined and configured using automated tools? - Whether SLA monitoring reports are generated and sent to senior management on periodic basis and relevant actions are taken?
5d	**INCIDENT MANAGEMENT**	**Security Incident Management**	**Security Incident Management:** - Whether management has defined and documented procedures for identifying security related incidents by monitoring logs generated by various IT assets such as

			Operating Systems, Databases, Network Devices, etc.? - Whether security incidents / events are detected, classified, investigated and resolved in a timely manner? - Whether periodic reports are published for various identified Security incidents? Whether the logging facilities and log information are protected from tampering and unauthorized access? - Whether security incidents are reported to SEBI in the prescribed format within stipulated timelines?
6	**BACKUP & RECOVERY**		**BACKUP & RECOVERY**
6a	**BACKUP & RECOVERY**	**Backup Administration**	**Backup Administration:** - Whether documented policies and procedures exist for backup scheduling, implementation and monitoring capturing version history and approval history? - Whether regular/ periodic back up of relevant data and programs is taken as per the approved backup policies and frequency [e.g., daily, weekly, etc.] configured via backup tool? - Whether access to backup tools is restricted to authorized personnel? - Whether modifications to backup schedule are performed through the formal change management process? - Whether appropriate data is backed up including at a minimum database records, audit trails, reports, user activity logs, transaction history, alert logs, etc.? - Whether execution of backups are monitored for successful completion and failures are investigated and closed?
6b	**BACKUP & RECOVERY**	**Backup Storage**	**Backup Storage:** - Whether backup tapes are stored onsite in a secure fireproof storage? - Whether access to onsite backups are limited to authorized personnel? - Whether backup tapes are sent for offsite storage on a periodic basis? - Whether offsite storage of tapes is monitored on a periodic basis?
6c	**BACKUP & RECOVERY**	**Restoration**	**Restoration:** - Whether restoration testing is performed on a periodic basis and issues, if any are resolved? - Whether request based restorations are performed only after obtaining approvals from business head?
7	**JOB PROCESSING**		**JOB PROCESSING**
7a	**JOB PROCESSING**	**Job Processing**	**Job Processing:** - Whether documented policies and procedures exist for automated job scheduling, implementation and monitoring capturing version history and approval history? - Whether automated jobs are processed as per the approved policies and frequency [e.g., daily, weekly, etc.] and configured via automated tool? - Whether access to job processing tools is restricted to authorized personnel?

			- Whether modifications to job schedules are performed through the formal change management process? - Whether execution of automated jobs are monitored for successful completion and failures are investigated and closed?
8	**BUSINESS CONTINUITY PLANNING (BCP) & DISASTER RECOVERY (DR)**		**BUSINESS CONTINUITY PLANNING (BCP) & DISASTER RECOVERY**
8a	**BUSINESS CONTINUITY PLANNING (BCP) & DISASTER RECOVERY (DR)**	**BCP Organization**	**BCP Organization:** - Whether the organization has a BCP Committee that provides oversight on BCP planning and functioning in the organization? - Whether the organization has a dedicated BCP Head or Coordinator overall responsible for development of the enterprise BCP framework in conjunction with internal and external facing functions within the organization through a defined process? - Whether the organization has a dedicated BCP Team or Crisis Management team to execute the BCP plan, when required. Does the BCP team have representations from various functions and locations of the organization? - Whether roles and responsibilities of all members of the BCP organization are defined and documented?
8b	**BUSINESS CONTINUITY PLANNING (BCP) & DISASTER RECOVERY (DR)**	**BCP Methodology and Plan**	**BCP Methodology and Plan:** - Whether the organization has a defined and documented BCP methodology which is approved by the BOD? - Whether the BCP methodology includes a process wise approach for development and maintenance of the BCP framework including Business Impact Analysis (BIA), Risk Assessment (RA), BCP Strategy, and BCP Plan? - Whether a documented BCP plan exists and is approved by the BOD? - Whether the BCP is developed based on the approved methodology and includes at a minimum the following: a. Organization's strategy for BCP b. Inputs from BIA and RA conducted c. BCP / DR procedures d. Conditions for activating plans e. BCP Team and responsibilities f. Maintenance schedules g. Awareness and education activities h. Resumption procedures i. Responsibilities of employees j. Emergency and fall back procedures
8c	**BUSINESS CONTINUITY PLANNING (BCP) &**	**BCP Plan**	**BCP Plan:** - Whether a BIA is conducted including identification of critical processes within the organization and their dependencies on other processes, vendor dependencies

	DISASTER RECOVERY (DR)		and resources. Whether Recovery Time Objective (RTO) and Recovery Point Objective (RPO) has been calculated as part of the BIA. Whether the BIA is approved by the business, technology and risk teams? - Whether a Risk Assessment is conducted for all critical processes identified in the BIA including identification of risks and threats and their impact, probability and priority. Whether the RA is conducted across parameters including people, processes and technology. Has the organization identified and implemented appropriate procedures and systems for risk mitigation? - Whether a documented BCP plan exists and is approved by the BOD. Whether the BCP is developed based on the approved methodology and includes at a minimum the following: a. Organization's strategy for BCP b. Inputs from BIA and RA conducted c. BCP / DR procedures d. Conditions for activating plans e. BCP Team and responsibilities f. Maintenance schedules g. Awareness and education activities h. Resumption procedures i. Responsibilities of employees j. Emergency and fall back procedures k. Procedures to be followed in the event of natural calamities and disasters that have a wide area or long term impact
8d	**BUSINESS CONTINUITY PLANNING (BCP) & DISASTER RECOVERY (DR)**	**BCP/ DR testing**	**BCP/ DR testing:** - Whether the BCP/ DR plan is reviewed on an yearly basis or in case of a major change in business or infrastructure? - Whether the defined BCP/ DR plan is tested through appropriate strategies including table-top reviews, simulations, DR drills, alternate site recovery testing, system recovery, etc. involving all aspects of people, process and technology?
8e	**BUSINESS CONTINUITY PLANNING (BCP) & DISASTER RECOVERY (DR)**	**BCP/ DR Communication and training**	**BCP/ DR Communication and training:** - Whether the organization has established appropriate procedures for BCP training and update for the BCP team? - Whether the BCP plan is communicated to all users internal as well as external with detailed description of roles, responsibilities and dependencies?
8f	**BUSINESS CONTINUITY PLANNING (BCP) & DISASTER RECOVERY (DR)**	**DR Plan**	**DR Plan:** - Whether the organization has documented a DR plan including recovery procedures to be followed in the event of disasters? - Has the organization identified and implemented a DR Site which is a replica of the production site? Has the organization implemented procedures for maintaining the DR readiness and support infrastructure to be relied upon in the event of a disaster? Have redundancies been built into systems and processes? - Are relevant system architecture documents prepared and approved representing infrastructure, hardware and software components at the primary and DR sites?

9	**BUSINESS CONTROLS**		**BUSINESS CONTROLS**
9a	**BUSINESS CONTROLS**	**Master Controls (Investment management, Front Office, Middle Office, Back Office, Fund Accounting, Registrar & Transfer Agent)**	**Master Controls (Investment management, Front Office, Middle Office, Back Office, Fund Accounting and Registrar & Transfer Agent):** - Whether new schemes/ funds are created in the system through an automated maker checker mechanism and based on the Scheme Information Documentation (SID) and information received from authorized sources? - Whether new customer accounts are created and assigned schemes/ funds based on the agreement signed with the customers? - Whether access to create/ update/ delete any master data (Customer/ Scheme/ Securities/ Broker/ Subscriptions/ Redemptions etc.) is restricted only to the authorized individuals? - Whether changes to masters are performed through an automated maker checker mechanism? - Whether system has the capability to capture audit trails/ logs of all changes, updation, and activities performed? - Whether update of security prices is controlled and is updated only from authorized automated/ manual sources?
9b	**BUSINESS CONTROLS**	**Front Office and Back Office Operations**	**Front Office and Back Office Operations:** - Whether appropriate segregation of duties is maintained between users having access to front office and back office system? - Whether controls exist over data integrity and accuracy on integration between the front office and back office system? - Whether system does not allow cancellation of deal order once the deal is confirmed in the system? - Whether trade settlement process is performed by authorized personnel through an automated maker checker mechanism? - Whether system allocates trades to the schemes as per defined policy?
9c	**BUSINESS CONTROLS**	**Risk Management (Middle Office)**	**Risk Management (Middle Office):** - Whether a documented risk management policy exists defining deal, counterparty wise limits, securities, etc. and the same is approved by the BOD? - Whether hard limits (beyond which system does not allow booking) and soft limits (for which system provides warnings) have been configured in the system in line with the risk management policy? - Whether there are controls defined to monitor and generate alerts/ reports in case of breach of predefined SEBI and Compliance limits defined at scheme/ fund level? - Whether system monitors the adherence to predefined rights/ limits assigned to Fund Manager at scheme/ fund level? - Whether systemic checks are performed for prohibiting blacklisted securities if entered by Dealers for Trades?

			- Whether the system monitors adherence to broker limits defined? - Whether appropriate field level validations and mandatory checks are built in the system to identify and appropriate expenses to individual schemes? - Whether the system monitors adherence to guidelines specified in the Ninth Schedule of the Mutual Fund Regulations with respect to accounting policies? - Whether the system monitors adherence to policies related to documentation of rationale for valuation including inter-scheme transfers?
9d	**BUSINESS CONTROLS**	**Investor Servicing (Registrar & Transfer Agent)**	**Investor Servicing (Registrar & Transfer Agent):** - Whether automated maker checker controls have been implemented for processing subscription and redemption requests? - Whether appropriate field level validations and mandatory checks are built in the system during subscription and redemption? - Whether the system has the capability to maintain the record of all types of transactions executed on behalf of the investor for specific scheme/ investment? - Whether the system has appropriate controls on brokerage computation and payouts?
9e	**BUSINESS CONTROLS**	**Fund Accounting**	**Fund Accounting:** - Whether NAV calculations, if automated are accurately calculated? - Whether end of day reconciliations (cash recon, portfolio recon, pricing recon, etc.) are performed to ensure no deals are missed from reporting to the fund accountant for processing and complete data is processed for safekeeping? - Whether details of the expenses accrued by the client (Management fees, audit etc.) are updated appropriately and accurately and maker-checker control exists? - Whether income related transactions are updated in the system appropriately and accurately? - Whether corporate actions are applied accurately and completely? - Whether NAV is accurately computed by Fund Accountant and the same is released to client, press, R&TA AMFI appropriately?
9f	**BUSINESS CONTROLS**	**Reporting**	**Reporting:** - Does the organization have list of regulatory and standard operational reports? - Has organization implemented reasonable controls over report generation with respect to accuracy and completeness?
9g	**BUSINESS CONTROLS**	**Custody of mutual fund scheme assets (Custodian)**	**Custody of mutual fund scheme assets (Custodian):** - Whether automated maker checker controls have been implemented for processing of receipt and delivery of securities, collection of income, distribution of dividends and segregation of assets between schemes and settlements between schemes?

			-Whether appropriate field level validations and mandatory checks are built in the system for receipt and delivery of securities, collection of income, distribution of dividends and segregation of assets between schemes and settlements between schemes? - Whether the system has the capability to maintain the record of all types of transactions executed on behalf of the client for specific scheme/ investment? - Whether end of day reconciliations (cash recon, portfolio recon, pricing recon, etc.) are performed to ensure whether all securities have been gone to the correct schemes in time? - Whether the system monitors adherence to controls related to significant accounting and valuation policies? - Whether the system monitors adherence to compliance with SEBI guidelines and PMLA guidelines?

ANNEXURE 9: PRODUCT LABELLING IN MUTUAL FUND SCHEMES – RISK-o-METER[8]

Risk level of a scheme shall be evaluated using the following methodology:

1. The underlying securities of a scheme shall be assigned a value for each of the parameters based on which the risk-o-meter value will be calculated.

2. For the purpose of evaluation of risk level, AUM of the security forming part of the scheme portfolio shall be as on last day of the given month.

3. The evaluation of risk parameters are as detailed below:

i. Debt securities

a) Credit Risk

- Debt securities of schemes shall be valued for credit risk as follows:

TABLE 1	
Credit rating of the Instrument	**CREDIT RISK VALUE**
G-Sec/AAA/SDL/ TREPS	1
AA+	2
AA	3
AA-	4
A+	5
A	6
A-	7
BBB+	8
BBB	9
BBB-	10
Unrated	11
Below investment grade	12

- Based on the weighted average value of each instrument (weights based on the AUM), credit risk value of the portfolio shall be assigned.
- The price of debt instrument to be considered for calculating AUM shall include the accrued interest i.e. dirty price.

[8] SEBI Circular no. SEBI/HO/IMD/DF3/CIR/P/2020/197 dated October 05, 2020

- For the above purpose, credit rating of the instrument as on last day of the month shall be considered.

b) Interest Rate Risk

- Interest rate risk shall be valued using Macaulay Duration of the Portfolio:

TABLE 2	
Macaulay Duration of the portfolio (years)	**INTEREST RATE RISK VALUE**
≤ 0.5	1
> 0.5 to ≤ 1	2
> 1 to ≤ 2	3
> 2 to ≤ 3	4
> 3 to ≤ 4	5
> 4	6

- For the above purpose, Macaulay Duration of an instrument as on last day of the month shall be considered.

c) Liquidity Risk

- For measuring liquidity risk of the schemes, listing status, credit rating, structure of debt instruments is considered.
- Liquidity risk of the debt securities shall be valued as follows:

TABLE 3	
Instrument	**LIQUIDITY RISK VALUE**
TREPS/G-Sec/AAA rated PSU/SDLs	1
Listed AAA rated debt securities without bespoke structures/ structured obligations, credit enhancements or embedded options*	2
Listed AA+ rated debt securities without bespoke structures/ structured obligations, credit enhancements or embedded options*	3
Listed AA rated debt securities without bespoke structures/ structured obligations, credit enhancements or embedded options*	4
Listed AA- rated debt securities without bespoke structures/ structured obligations, credit enhancements or embedded options*	5
Listed A+ rated debt securities without bespoke structures/ structured obligations, credit enhancements or embedded options*	6

TABLE 3	
Instrument	**LIQUIDITY RISK VALUE**
Listed A rated debt securities without bespoke structures/ structured obligations, 7credit enhancements or embedded options*	7
Listed A- rated debt securities without bespoke structures/ structured obligations, credit enhancements or embedded options*	8
Listed BBB+ rated debt securities without bespoke structures/ structured obligations, credit enhancements or embedded options*	9
Listed BBB rated debt securities without bespoke structures/ structured obligations, credit enhancements or embedded options*	10
Listed BBB- rated debt securities without bespoke structures/ structured obligations, credit enhancements or embedded options*	11
AAA rated debt securities with any one of the following features*- • unlisted • bespoke structure • structured obligation • credit enhancement • embedded options	3
AA + rated debt securities with any one of the following features*- • unlisted • bespoke structure • structured obligation • credit enhancement • embedded options	4
AA rated debt securities with any one of the following features*- • unlisted • bespoke structure • structured obligation • credit enhancement • embedded options	5
AA- rated debt securities with any one of the following features*- • unlisted • bespoke structure • structured obligation • credit enhancement • embedded options	6
A+ rated debt securities with any one of the following features*-	7

TABLE 3	
Instrument	**LIQUIDITY RISK VALUE**
• unlisted • bespoke structure • structured obligation • credit enhancement • embedded options	
A rated debt securities with any one of the following features*- • unlisted • bespoke structure • structured obligation • credit enhancement • embedded options	8
A- rated debt securities with any one of the following features*- • unlisted • bespoke structure • structured obligation • credit enhancement • embedded options	9
BBB+ rated debt securities within investment grade with any one of the following features*- • unlisted • bespoke structure • structured obligation • credit enhancement • embedded options	10
BBB rated debt securities within investment grade with any one of the following features*- • unlisted • bespoke structure • structured obligation • credit enhancement • embedded options	11
BBB- rated debt securities within investment grade with any one of the following features*- • unlisted • bespoke structure • structured obligation • credit enhancement • embedded options	12
AAA rated debt securities with more than one of the following features*- • unlisted • bespoke structure	4

TABLE 3	
Instrument	**LIQUIDITY RISK VALUE**
• structured obligation • credit enhancement • embedded options	
AA + rated debt securities with more than one of the following features*- • unlisted • bespoke structure • structured obligation • credit enhancement • embedded options	5
AA rated debt securities with more than one of the following features*- • unlisted • bespoke structure • structured obligation • credit enhancement • embedded options	6
AA- rated debt securities with more than one of the following features*- • unlisted • bespoke structure • structured obligation • credit enhancement • embedded options	7
A+ rated debt securities with more than one of the following features*- • unlisted • bespoke structure • structured obligation • credit enhancement • embedded options	8
A rated debt securities with more than one of the following features*- • unlisted • bespoke structure • structured obligation • credit enhancement • embedded options	9
A- rated debt securities with more than one of the following features*- • unlisted • bespoke structure • structured obligation • credit enhancement	10

TABLE 3	
Instrument	**LIQUIDITY RISK VALUE**
• embedded options	
BBB+ rated debt securities with more than one of the following features*- • unlisted • bespoke structure • structured obligation • credit enhancement • embedded options	11
BBB rated debt securities with more than one of the following features*- • unlisted • bespoke structure • structured obligation • credit enhancement • embedded options	12
BBB- rated debt securities with more than one of the following features*- • unlisted • bespoke structure • structured obligation • credit enhancement • embedded options	13
Below investment grade and unrated debt securities	14
*Or any other structure / feature which increase the liquidity risk of the instrument.	

- Liquidity Risk Value of a portfolio shall be assigned based on the weighted average of such values (weights based on the AUM) of each instrument.
- For the above purpose, instruments held by the scheme as on last day of the month shall be considered.

d) Risk value for the debt portfolio shall be simple average of credit risk value, interest rate risk value and liquidity risk value. However, if the liquidity risk value is higher than the average of credit risk value, liquidity risk value and interest rate risk value then the value of liquidity risk shall be considered as risk value of the debt portfolio.

e) For investment by mutual funds in instruments having short term ratings, the liquidity risk value and the credit risk value shall be based on the lowest long term rating of the instrument of the same issuer as shown above (in order to follow conservative approach) across credit rating agencies. However, if there is no long term rating of the same issuer, then based on credit rating mapping most conservative long term rating shall be taken for a given short term rating.

ii. Equity

a) Market Capitalisation

- Following values shall be assigned to the security for market capitalisation parameter:

TABLE 4	
Market Cap of the underlying security	**MARKET CAPITALISATION VALUE**
Large cap	5
Mid cap	7
Small cap	9

- The market capitalisation data as published by AMFI on six-monthly basis shall be considered.
- Based on the weighted average of the above Market Capitalisation values of each security (weights being AUM of the security), Market Capitalisation Value of a portfolio shall be assigned.

b) Volatility

- Following values shall be assigned to the security based on its volatility:

TABLE 5	
Daily Volatility of the Security price (based on the past two years price of the security)	**VOLATILITY VALUE**
≤ 1%	5
> 1%	6

- Based on the weighted average of above volatility values of each security (weights being AUM of the security), Volatility Value of a portfolio shall be assigned.

  If an instrument is traded on multiple stock exchanges, then the most conservative volatility value across stock exchanges for a given month shall be considered.

c) Impact Cost (Liquidity Measure)

- Impact cost shall be considered as a measure for liquidity. Based on the average impact cost of the security for previous three months including the month under consideration following values shall be assigned:

TABLE 6	
Average Impact Cost of the Security for the month	**IMPACT COST VALUE**
≤ 1%	5
>1 % to ≤ 2%	7
> 2%	9

- Based on the weighted average of impact cost values of each security (weights being AUM of the security), impact cost value of a portfolio shall be assigned.
- If an instrument is traded on multiple stock exchanges, then the impact cost shall be based on average value of impact costs across stock exchanges for a given month.

d) For investment in IPOs or recently listed securities**,** the following process shall be adopted for arriving at weighted average value for Risk-o-meter:

- Market Capitalisation value: Market capitalisation of a security as on the last trading day of the month shall be compared with that of the market capitalisation of the threshold for large cap, mid cap and small cap as published by AMFI and then market capitalisation parameter of risk shall be valued based on the Table 4 mentioned above.

- Volatility value: For the first three months of trading of a security, the value for volatility shall be assigned as 6. From the subsequent months, volatility shall be calculated based on the available security prices as mentioned at Table 5 above.
- Impact cost value: For the first three months of trading of a security, the impact cost value shall be assigned as 5. From the subsequent month, impact cost value shall be as mentioned in Table 6 above.

e) Risk value for equity portfolio shall be simple average of market capitalisation value, volatility value and impact cost value.

iii. Equity Derivatives

- For hedging positions, the underlying security held and its corresponding derivative instrument shall not be included for arriving at risk value. For instance, if XYZ security in cash market is being hedged by its futures instrument, then the XYZ cash market security and short futures position in XYZ security both shall not be considered for arriving at risk value.
- If the quantity of derivative positions taken for hedging purposes are in excess of the underlying position against which the hedging position has been taken, the excess position shall be included while calculating the risk value.

iv. Index Futures and Stock Futures

- For index and stock futures, following values are to be assigned:

TABLE 7	
Value for Index / Stock futures	**INDEX / STOCK FUTURES VOLATILITY VALUE**
≤ NIFTY near month futures annualized volatility	5
> NIFTY near month futures annualized volatility	6

- Based on the weighted average of above values of each security (weights being AUM of the security), the risk value shall be assigned to the portfolio.

v. Index Options and Stock Options

- For index and stock options, following values are to be assigned:

TABLE 8	
Value for Index / Stock options	**INDEX / STOCK OPTIONS' IMPLIED VOLATILITY VALUE**
≤ India VIX	5
> India VIX	6

- Based on the weighted average of above values of each security (weights being AUM of the security), the risk value shall be assigned to the portfolio.

vi. Other derivative instruments

- If the derivative instrument is used for hedging, then the hedging instrument shall not be included for calculating the risk value only if the quantity of derivative instrument is less than or equal to the quantity of underlying/instrument being hedged. If the derivative instrument position is in excess of the underlying then the excess position shall be considered while calculating the risk value.
- If Interest rate swaps (IRS) are being used for hedging purpose, then IRS shall not be considered for arriving at the risk value.
- For investment in other derivative instruments, such instruments shall be valued as under:

TABLE 9	
Daily Volatility of the instrument	**VOLATILITY VALUE**
≤ 1%	5
>1%	6

- Volatility calculated above is based on daily close prices of past three months of the instrument.

- Based on the weighted average of above values of each security (weights being AUM of the security), the risk value shall be assigned to the portfolio.

vii. REITs & InvITs

- Investment by schemes in REITs and InvITs shall be valued as 7 from risk perspective.
- Based on the weighted average of each security (weights being AUM of the security), the risk value shall be assigned to the portfolio.

viii. Commodities (Gold/Silver) in which mutual funds are permitted to invest:[9]

- Investment in Gold/Silver and gold/silver related instruments by mutual fund schemes shall be assigned a risk score corresponding to the annualized volatility of the price of said commodity. The annualized volatility shall be computed quarterly based on past 15 years' prices of benchmark index of the said commodity and risk score for the commodity shall be in terms of the following table:

Annualized volatility	Risk value on risk-o-meter (Risk)
<10%	3 (Moderate)
10-15%	4 (Moderately High)
15-20%	5 (High)
>20%	6 (Very high)

Illustration: If price of gold has annualized volatility of 18% based on price of gold of past 15 years, then Gold and gold related instruments will have risk value of 5 (High) on risk-o-meter.

[9] SEBI Circular No. SEBI/HO/IMD/IMD-II DOF3/P/CIR/2022/49 dated April 11, 2022

ix. Foreign Securities

- Investment by schemes in foreign securities shall be valued as 7 from risk perspective.
- Based on the weighted average of each security (weights being AUM of the security), the risk value shall be assigned to the portfolio.

x. Mutual Fund Schemes:

- For schemes holding units of other mutual fund schemes, the following values shall be assigned basis the risk-o-meter of underlying schemes:

TABLE 10	
Risk as per risk-o-meter	**Value**
Low	1
Low to Moderate	2
Moderate	3
Moderately High	4
High	5
Very High	6

- The risk value for investment in overseas mutual fund units or ETFs shall be 7.
- Based on the weighted average of each mutual fund scheme held (weights being AUM of the scheme), the risk value shall be assigned to the portfolio.

xi. Cash and Net Current Assets:

- Cash and Net Current Assets, shall be valued as 1 from risk perspective.

4. **Risk-o-meter value**

- Based on the above calculations, the risk value arrived upon shall be mapped to the risk level mentioned in the table below and the same may be depicted in the risk-o-meter:

TABLE 11	
Risk Value	**RISK LEVEL AS PER RISK-O-METER**
≤ 1	Low
>1 to ≤ 2	Low to Moderate
>2 to ≤ 3	Moderate
>3 to ≤ 4	Moderately High
>4 to ≤ 5	High
>5	Very High

5. **Illustrations**:

In order to illustrate the above process, following are a few illustrations:

1. Debt scheme

- Consider a bond scheme category having 10 debt securities with following attributes:
    - At the portfolio level, the average Macaulay Duration is 1.41

TABLE 12			
Securities held by the scheme	**Weight as % of AUM**	**Credit rating**	**Structure**
A	10%	AAA - PSU	No additional feature/structure
B	10%	AA-	Unlisted and has structured obligation
C	10%	A	No additional feature/structure
D	10%	BBB+	No additional feature/structure
E	10%	AA	Has credit enhancement
F	10%	AA+	Is bespoke and unlisted
G	10%	A	No additional feature/structure
H	10%	AA	No additional feature/structure
I	10%	AAA	No additional feature/structure
J	10%	TREPS	-

DEBT- Security A to J

- Based on the above portfolio, following shall be parameter based valuing of securities held by the scheme:

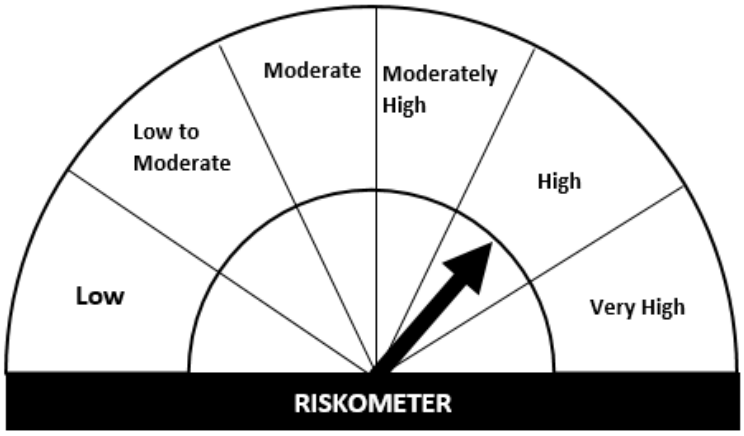
TABLE 13				
Securities held by the scheme	**Weight as % of AUM**	**Credit Risk value**	**Interest Rate Risk Value**	**Liquidity risk value**
A	10%	1		1
B	10%	4		7
C	10%	6		7
D	10%	8		9
E	10%	3		5
F	10%	2		5
G	10%	6		7
H	10%	3		4
I	10%	1		2
J	10%	1		1
TOTAL*		3.5	3	4.8

*Total is calculated as weighted average with weights based on AUM of the instrument in the scheme as under:

TABLE 14		
Parameter	**Average**	**Value**
Credit risk	0.1 X 1 + 0.1 X 4 + 0.1 X 6 + 0.1 X 8 + 0.1 X 3 + 0.1 X 2 + 0.1 X 6 + 0.1 X 3 + 0.1 X 1 + 0.1 X 1	3.5
IR Risk	1 x 3	3
LR value	0.1 X 1 + 0.1 X 7 + 0.1 X 7 + 0.1 X 9 + 0.1 X 5 + 0.1 X 5 + 0.1 X 7 + 0.1 X 4 + 0.1 X 2 + 0.1 x 1	4.8
Simple Average		3.8

PORTFOLIO RISK-O-METER VALUE:

- Simple average of the above three parameters comes out to 3.8 ([3.5+3+4.8]/3)
- Since the liquidity risk value of 4.8 is higher than the average value of above three parameters i.e. 3.8, the risk value assigned to the scheme will be 4.8. Hence, the risk level as per Risk-o-meter is High.
- Therefore, risk-o-meter for the abovementioned debt scheme would be **High,** and shall be as depicted below:



2. Equity scheme

- Consider an Equity scheme having 10 equity securities with following attributes:

TABLE 15				
Securities held by the scheme	**Weight as % of AUM**	**Market Cap**	**Volatility**	**Impact cost**
A	10%	Large Cap	0.01%	0.2%
B	10%	Large Cap	1.5%	0.3%
C	10%	Mid cap	2.5%	1.5%
D	10%	Mid cap	1.5%	1.2%
E	10%	Mid cap	2%	1.9%
F	10%	Mid cap	1.5%	1.2%
G	10%	Large Cap	0.005%	0.7%
H	10%	IPO	-	-
I	10%	Small Cap	1.7%	2.5%
J	10%	Cash	-	-

- Based on the above portfolio, following shall be the scoring of the securities held by the scheme across parameters:

EQUITY – Security A to I

TABLE 16				
Securities held by the scheme	**Weight as % of AUM**	**Market Cap Value**	**Volatility Value**	**Impact cost Value**
A	10%	5	5	5
B	10%	5	6	5
C	10%	7	6	7
D	10%	7	6	7
E	10%	7	6	7
F	10%	7	6	7
G	10%	5	5	5
H*	10%	7	6	5
I	10%	9	6	9
TOTAL	**90%**	**6.6**	**5.8**	**6.3**

* Assuming the market cap of the security at the time of listing is falling under Mid cap as per the market cap data published by AMFI, a value of 7 is considered. Volatility value and Impact cost value are considered as 6 and 5 respectively.

- The TOTAL mentioned above is calculated as under:

TABLE 17		
Parameter	**Average**	**Value**
Market Cap	0.1 X 5 + 0.1 X 5 + 0.1 X 7 + 0.1 X 7 + 0.1 X 7 + 0.1 X 7 + 0.1 X 5 + 0.1 X 7 + 0.1 X 9	6.6
Volatility Value	0.1 X 5 + 0.1 X 6 + 0.1 X 6 + 0.1 X 6 + 0.1 X 6 + 0.1 X 6 + 0.1 X 5 + 0.1 X 6 + 0.1 X 6	5.8
Impact cost value	0.1 X 5 + 0.1 X 5 + 0.1 X 7 + 0.1 X 7 + 0.1 X 7 + 0.1 X 7 + 0.1 X 5 + 0.1 X 5 + 0.1 X 9	6.3
Simple Average		6.2

- Simple average of the above three parameters comes out to 6.2 [(6.6+5.8+6.3)/3]

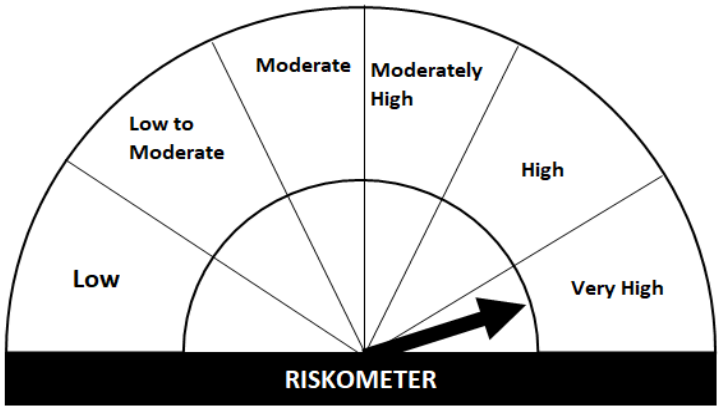
CASH – Component J

- Further, cash component is valued as 1.

PORTFOLIO RISK-O-METER VALUE:

- Hence, the average for the total portfolio is 6.2 + 0.1 x 1 = 6.3

- Since the value of risk is higher than 5, it shall fall into range of Very High Risk.
- Therefore, risk-o-meter for the abovementioned equity scheme would be **Very High,** and shall be as depicted below:



3. Multi asset scheme:

- Consider a Multi Asset category scheme having 10 securities with following attributes:

TABLE 18					
Type of security	**Securities held by the scheme**	**Weight as % of AUM**	**Market Cap**	**Volatility**	**Impact cost**
Equity	A	20%	Large Cap	0.01%	0.2%
Equity	B	10%	Large Cap	1.5%	0.3%
Equity	C	10%	Mid cap	2.5%	1.5%
Type of security	**Securities held by the scheme**	**Weight as a % of AUM**	**Credit rating**	**Macaulay Duration**	**Structure**
Debt	D	10%	A	2.6	No additional feature/structure
Debt	E	10%	AA	2.1	No additional feature/structure
Debt	F	10%	AAA	2.8	No additional

TABLE 18					
					feature/structure
TREPS	G	10%	-	-	-
Gold ETF	H	10%	-	-	-
REITS	I	10%	-	-	-
Interest rate swap (IRS)	J	-20%			

- As interest rate swap instrument was used for hedging, it is not included while calculating the risk value.
- Macaulay Duration of debt scheme portfolio (D, E & F) is 2.5 years
- Based on the above portfolio, following shall be the valuing of the securities held by the scheme across parameters:

TABLE 19				
Securities held by the scheme	**Weight as % of AUM**	**Market Cap Value**	**Volatility Value**	**Impact cost Value**
A	20%	5	5	5
B	10%	5	6	5
C	10%	7	6	7
Securities held by the scheme	**Weight as a % of AUM**	**Credit Risk value**	**Interest rate risk value**	**Liquidity risk value**
D	10%	6		7
E	10%	3		4
F	10%	1		2
G	10%	1		1

EQUITY- Security A, B and C

TABLE 20				
Securities held by the scheme	**Weight as % of AUM**	**Market Cap Value**	**Volatility Value**	**Impact cost Value**
A	20%	5	5	5
B	10%	5	6	5
C	10%	7	6	7

TABLE 21		
Parameter	**Average**	**Value**
Market Cap	0.2 X 5 + 0.1 X 5 + 0.1 X 7	2.2
Volatility Value	0.2 X 5 + 0.1 X 6 + 0.1 X 6	2.2
Impact cost value	0.2 X 5 + 0.1 X 5 + 0.1 X 7	2.2
Simple Average		2.2

DEBT- Security D, E, F and G

TABLE 22				
Securities held by the scheme	**Weight as a % of AUM**	**Credit Risk value**	**Interest rate risk value**	**Liquidity risk value**
D	10%	6		7
E	10%	3		4
F	10%	1		2
G	10%	1		1

TABLE 23		
Parameter	**Average**	**Value**
Credit risk	0.1 X 6 + 0.1 X 3 + 0.1 X 1 + 0.1 X 1	1.1
IR Risk	0.4 x 4	1.6
LR value	0.1 X 7 + 0.1 X 4 + 0.1 X 2 + 0.1 X 1	1.4
Simple Average		1.37

- For debt component, Simple average of the three parameters comes out to 1.37.
- Since the liquidity risk value of 1.4 is higher than the average value of above three parameters i.e. 1.37, the risk value assigned to the scheme will be 1.4.

GOLD and REITS - H and I

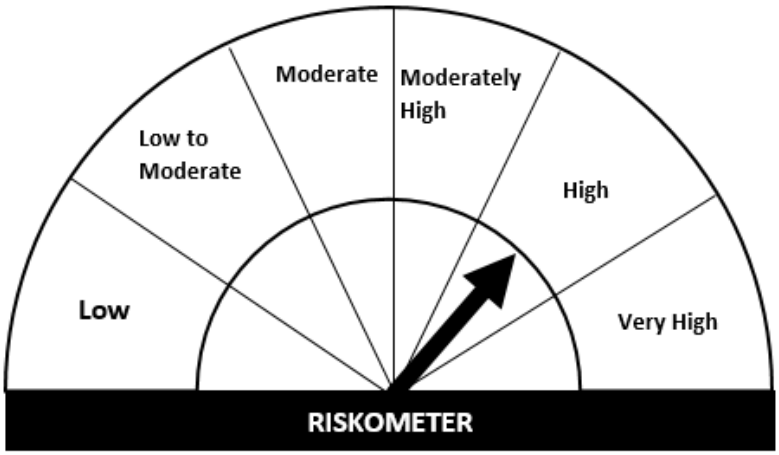
TABLE 24			
Securities held by the scheme	**Weight as a % of AUM**	**Risk Value**	**Value**
H	10%	4	0.4
I	10%	7	0.7

PORTFOLIO RISK-O-METER VALUE:

- The final weighted average risk value for the portfolio is as under:

  2.2 + 1.4 + 0.4 + 0.7 = 4.7

- Since the value of risk is higher than 4, it shall fall into range of High Risk.
- Therefore, risk-o-meter for the abovementioned scheme would be **High**, and shall be as depicted below.



ANNEXURE 10: STEWARDSHIP CODE FOR ALL MUTUAL FUNDS IN RELATION TO THEIR INVESTMENT IN LISTED EQUITIES[10]

- **Principle 1**

  Institutional Investors should formulate a comprehensive policy on the discharge of their stewardship responsibilities, publicly disclose it, review and update it periodically.

Guidance

Stewardship responsibilities include monitoring and actively engaging with investee companies on various matters including performance (operational, financial, etc.), strategy, corporate governance (including board structure, remuneration, etc.), material environmental, social, and governance (ESG) opportunities or risks, capital structure, etc. Such engagement may be through detailed discussions with management, interaction with investee company boards, voting in board or shareholders meetings, etc.

Every institutional investor should formulate a comprehensive policy on how it intends to fulfill the aforesaid stewardship responsibilities and disclose it publicly. In case any of the activities are outsourced, the policy should provide for the mechanism to ensure that in such cases, stewardship responsibilities are exercised properly and diligently.

The policy should be reviewed and updated periodically and the updated policy should be publicly disclosed on the entity's website. A training policy for personnel involved on implementation of the principles is crucial and may form a part of the policy.

[10] SEBI Circular no. CIR/CFD/CMD1/ 168 /2019 dated December 24, 2019

- **Principle 2**

  Institutional investors should have a clear policy on how they manage conflicts of interest in fulfilling their stewardship responsibilities and publicly disclose it.

Guidance

As a part of the aforesaid comprehensive policy, institutional investors should formulate a detailed policy for identifying and managing conflicts of interest. The policy shall be intended to ensure that the interest of the client/beneficiary is placed before the interest of the entity. The policy should also address how matters are handled when the interests of clients or beneficiaries diverge from each other.

The conflict of interest policy formulated shall, among other aspects, address the following:

1. Identifying possible situations where conflict of interest may arise. E.g. in case of investee companies being associates of the entity.
2. Procedures put in place by the entity in case such conflict of interest situations arise which may, *inter alia,* include:
    a. Blanket bans on investments in certain cases
    b. Having a *'Conflict of Interest'* Committee to which such matters may be referred to.
    c. Clear segregation of voting function and client relations/ sales functions.
    d. Policy for persons to recuse from decision making in case of the person having any actual/ potential conflict of interest in the transaction.
    e. Maintenance of records of minutes of decisions taken to address such conflicts.
3. Periodical review and update of such policy and public disclosure.

- **Principle 3**

  Institutional investors should monitor their investee companies.

Guidance

As a part of the aforesaid comprehensive policy, institutional investors should have a policy on continuous monitoring of their investee companies in respect of all aspects they consider important which shall include performance of the companies, corporate governance, strategy, risks etc.

The investors should identify the levels of monitoring for different investee companies, areas for monitoring, mechanism for monitoring etc. The investors may also specifically identify situations where they do not wish to be actively involved with the investee companies e.g. in case of small investments.

The investors should also keep in mind regulations on insider trading while seeking information from the investee companies for the purpose of monitoring.

Accordingly, the institutional investors shall formulate a policy on monitoring specifying, *inter-alia,* the following:

1. Different levels of monitoring in different investee companies. E.g. companies where larger investments are made may involve higher levels of monitoring vis-à-vis companies where amount invested in insignificant from the point of view of its assets under management.

2. Areas of monitoring which shall, inter-alia, include:
    a. Company strategy and performance - operational, financial etc.
    b. Industry-level monitoring and possible impact on the investee companies.
    c. Quality of company management, board, leadership etc.

d. Corporate governance including remuneration, structure of the board (including board diversity, independent directors etc.) related party transactions, etc.

e. Risks, including Environmental, Social and Governance (ESG) risks

f. Shareholder rights, their grievances etc.

3. Identification of situations which may trigger communication of insider information and the procedures adopted to ensure insider trading regulations are complied with in such cases.

- **Principle 4**

Institutional investors should have a clear policy on intervention in their investee companies. Institutional investors should also have a clear policy for collaboration with other institutional investors where required, to preserve the interests of the ultimate investors, which should be disclosed.

Guidance

Institutional investors should have a clear policy identifying the circumstances for active intervention in the investee companies and the manner of such intervention. The policy should also involve regular assessment of the outcomes of such intervention. Intervention should be considered even when a passive investment policy is followed or if the volume of investment is low, if the circumstances so demand.

Circumstances for intervention may, inter alia, include poor financial performance of the company, corporate governance related practices, remuneration, strategy, ESG risks, leadership issues, litigation etc.

The mechanisms for intervention may include meetings/discussions with the management for constructive resolution of the issue and in case of escalation

thereof, meetings with the boards, collaboration with other investors, voting against decisions, etc. Various levels of intervention and circumstances in which escalation is required may be identified and disclosed. This may also include interaction with the companies through institutional investor associations (E.g. AMFI). A committee may also be formed to consider which mechanism to be opted, escalation of matters, etc. in specific cases.

- **Principle 5**

  Institutional investors should have a clear policy on voting and disclosure of voting activity.

  Guidance

  To protect and enhance wealth of the clients/ beneficiaries and to improve governance of the investee companies, it is critical that the institutional investors take their own voting decisions in the investee company after in-depth analysis rather than blindly supporting the management decisions.

  This requires a comprehensive voting policy to be framed by the institutional investors including details of mechanisms of voting, circumstances in which voting should be for/against/abstain, disclosure of voting, etc. The voting policy, voting decisions (including rationale for decision), use of proxy voting/voting advisory services, etc. should be publicly disclosed.

  The voting policy shall, *inter-alia,* include the following:

  1. Mechanisms to be used for voting (e.g. e-voting, physically attending meetings, voting through proxy, etc.)

  2. Internal mechanisms for voting including:
     a. Guidelines on how to assess the proposals and take decision thereon

b. Guidelines on how to vote on certain specific matters/ circumstances including list of such possible matters/circumstances and factors to be considered for a decision to vote for/ against/ abstain

c. Formulation of oversight committee as an escalation mechanism in certain cases

d. Use of proxy advisors

e. Policy for conflict of interest issues in the context of voting

3. Disclosure of voting including:

a. Periodicity of disclosure

b. Details of actual voting for every proposed resolution in investee companies i.e. *For, Against or Abstain*

c. Rationale for voting

d. Manner of disclosure – e.g. in annual report to investors, quarterly basis on website etc.

4. In case of use of proxy voting or other voting advisory services, disclosures on:

a. Scope of such services

b. Details of service providers

c. Extent to which the investors rely upon/use recommendations made by such services

- **Principle 6**

Institutional investors should report periodically on their stewardship activities.

Guidance

Institutional investors shall report to their clients/ beneficiaries periodically on how they have fulfilled their stewardship responsibilities as per their policy in an easy-to-understand format.

However, it may be noted that the compliance with the aforesaid principles does not constitute an invitation to manage the affairs of a company or preclude a decision of the institutional investor to sell a holding when it is in the best interest of clients or beneficiaries.

Institutional investors shall report periodically on their stewardship activities in the following manner:

1. A report may be placed on website on implementation of every principle. Different principles may also be disclosed with different periodicities. E.g. Voting may be disclosed on quarterly basis while implementation of conflict of interest policy may be disclosed on an annual basis. Any updation of policy may be disclosed as and when done.
2. The report may also be sent as a part of annual intimation to its clients/ beneficiaries.

ANNEXURE 11: DECLARATION FORM FOR OPTING OUT OF NOMINATION[11]

To, Mutual Fund/ AMC's Name Mutual Fund/ AMC's Address	**Date:** D D D M M Y Y Y Y
Mutual Fund Folio Number	
Sole/First Holder Name	
Second Holder Name	
Third Holder Name	
I/We hereby confirm that I/We do not wish to appoint any nominee(s) for any mutual fund units held in my/ our mutual fund folio and understand the issues involved in non-appointment of nominee(s) and further are aware that in case of death of all the account holder(s), my/our legal heirs would need to submit all the requisite documents issued by Court or other such competent authority, based on the value of assets held in the mutual fund folio.	
Name and Signature of Unitholder(s) Unitholder (1) Signature: _____ Name: _____ Unitholder (2) Signature: _____ Name: _____ Unitholder (3) Signature: _____ Name: _____	

[11] SEBI Circular no. SEBI/HO/IMD/IMD-II DOF3/P/CIR/2022/82 dated June 15, 2022

ANNEXURE 12: GUIDELINES REGARDING THE MARKET MAKING FRAMEWORK[12]

1. Market Making in ETFs

The following broad points shall be considered while designing the market making framework in ETFs:

1.1. Obligations of AMC: Obligations shall, *inter-alia*, include:

1.1.1. AMCs to enter into agreement with at least two Market Makers (MMs) for each ETF.

1.1.2. AMCs may select MMs based on various criteria including experience in the capital market, capital adequacy, net worth, infrastructure, volume of business, etc.

1.2. Obligations and responsibilities of a Market Maker: Obligations shall, inter-alia, include:

1.2.1. **Quote:** MM shall be mandated to provide a two-way quote during such minimum time frame for which the MM may be required to make market. MM shall guarantee execution of orders at quoted price and quantity for quotes given by it.

1.2.2. **Minimum timeframe:** The minimum time frame for which the MM is required to make the market shall be 75% of the time during market hours of a trading day. Further, MM shall also be mandated to be present in the Best Buy/Sell order/quote for e.g. top 5 buy/sell order/quote.

1.3. Information to be collected from Stock Exchanges: AMCs to collect the following information from SEs on daily basis:

1.3.1. Total quantity traded by the MM in a particular ETF and its % trade to total quantity traded in the market of that ETF.

[12] SEBI Circular No. SEBI/HO/IMD/DOF2/P/CIR/2022/69 dated May 23, 2022

1.3.2. Minimum, Maximum and Median prices at which the MM has executed the trades.

1.3.3. Minimum, Maximum and Median spread at which the MM has provided the quotes.

1.4. Compensation of MM: The issue of compensation is to be decided between the AMC and the MM. It may have recourse to factors such as trading volume, bid-ask spread in units of ETFs, and such other information as may be required to formalize performance based incentive structure.

******