DSP
ASSET MANAGERS

Risk Management Framework and Policy

DSP
ASSET MANAGERS

Risk Management Framework and Policy for DSP Asset Managers

Introduction:

With the overall objective of management of key risks involved in mutual fund operations, SEBI on September 27, 2021, outlined a revised Risk Management Framework (RMF) to provide a set of principles or standards, which inter alia comprise the policies, procedures, risk management functions and roles & responsibilities of the management, the Board of Asset Management Company (AMC) and the Board of Trustees. The provisions of the circular come into effect from 1st April 2022.

The circular outlines the risk management framework standards; namely, the RMF should have the following characteristics

- Be structured, efficient and timely
- 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.
- 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.
- Be dynamic and flexible enough to identify new risks that emerge and make allowances for those risks that no longer exist
- Recognize that people and culture have an impact on its effectiveness, and accordingly the framework must communicate and consult with stakeholders throughout.
- Protect reputation

The objectives of RMF should assist the management and the Board of Directors of both AMC and Trustees in:

- Demonstrating high standards of due diligence in daily management
- Promoting proactive management and early identification of risk
- Assigning and increasing accountability and responsibility in the organization
- Managing risk within the tolerance limits defined in the RMF.

The RMF of mutual funds shall comprise the following components

- Governance and Organization
- Identification of Risks
- Measurement and Management of Risks
- Reporting of Risks and related Information

The policy on the RMF will be approved by the board of AMC and trustees.

The provisions of this policy shall also extend to its subsidiary companies, except where the applicable regulator's circulars, guidance, or regulations provide specific provisions, in which case those shall prevail.

The RMF will be reviewed in the event of material claims or litigations from customers or incidents, material findings from internal or external audits, adverse media attention impacting reputation risk, adverse observations from the regulator(s), key risk indicator breaches, new regulatory requirements, sector-relevant developments or incidents.

I. Governance and Organization

DSP Asset Managers has an independent risk management function. The risk management function is headed by the Chief Risk Officer who is responsible for the overall risk management of the mutual fund operation including the key risks. There is also a CXO level officer responsible for the risk management of specific functions of the AMC/Mutual Fund. The CXO will be the "Head of Department" of the respective function. However, for the overall risk management of the mutual fund, along with the management, both board of AMC and trustees are also responsible.

DSP Asset Managers has constituted Risk Management Committees (RMC) of the AMC and Trustees respectively comprising of relevant Board members (including independent director(s)) and any other invitees as may be identified by the Board. Chief Risk Officer ("CRO") would be a permanent invitee to the Risk Management Committees.

The respective Committee members shall decide and elect a chairperson for the committee. The Committee would be chaired by an Independent Director.

The Quorum of the Committees shall be a simple majority of the total committee members and at least one Independent Director will be part of the meeting.

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

The RMCs will meet at least once in a quarter or at shorter frequency as may be required on case-to-case basis.

Further KRAs for executives of AMC covering risk management have been included as a parameter for performance appraisal of all the officials of the AMC including the CEO and up to two levels below CEO with specific weightage assigned in the overall performance assessment.

Please find below the list of the indicative risk management related Key Roles and Responsibilities assigned to committees & executives under the framework guidance prescribed by SEBI vide circular SEBI/HO/IMD/IMD-1 DOF2/P/CIR/2021/630 September 27, 2021, and as amended later, which needs to be adhered to by all the committees & executives.

DSP
ASSET MANAGERS

Risk Management - Role of the Board of AMC and Trustees

1	Review and approve mandatory risk management policies and framework both at AMC and scheme level, including but not limited to: a) Risk Management Policy b) Investment policy c) Credit risk policy, d) Liquidity risk policy, e) Operational risk management policy (including Incident reporting and escalation matrix), f) Outsourcing policy, g) Cyber security and information security policy h) Business Continuity and Disaster Recovery Plan i) Such other policies as may be prescribed by SEBI from time to time Any modifications to the policies approved by the Executive Risk Management Committee ("ERMC") shall be reviewed by the RMC of AMC and Trustee
2	Review and approve the risk appetite, risk metric and tolerance limits for AMC and schemes.
3	Periodically review the risk appetite, risk metrics against actual risk of the AMC and scheme.
4	Review breaches to risk appetite and thresholds for risk matrix and approve the action plan for remediation
5	Define mechanism for risk reporting on a quarterly basis by ERMC to the RMC of the AMC and Trustees and review outcome and submission on a quarterly basis
6	Annually review and approve changes to the roles and responsibilities and Delegation of Power ("DoP") as placed by the ERMC
7	Periodically review material breaches in the code of conduct
8	Monitor and review the major findings, exceptions, deviations, resolution, strategies as recommended by the ERMC or previous RMCs for the existing and emerging risks identified
9	Review of the exceptions in a) Results of stress testing (investment, credit and liquidity risks) b) Outliers identified during "Early Warning Signals" review c) Material alerts generated through the liquidity risks model at scheme level d) Material deviations, issues and corrective actions as a result of periodic RCSA review e) Other Dashboards and reports prepared by management highlighted to the ERMC f) Material Incidents and Events reported as per the Operating Event Management Policy and escalated by ERMC
10	Review reports on outsourced vendor highlighting risks emanating from them along with the remediation plans
11	Review and recommend the level and type of insurance cover against first- and third-party losses arising from errors and omissions
12	Review evaluation of the fraudulent incidents submitted by the ERMC
13	Formulate and approve a methodology for annual evaluation of the RMF, either through outsourced or by way of self-assessment.
14	Review the findings and action plan on the annual RMF compliance review prior to submission to SEBI in the half yearly SEBI report.
15	Approve Terms of Reference for Executive Risk Management Committee (ERMC)
16	Delegate critical matters to CEO or the Executive Risk Management Committee
17	Recommend reduction/ change in the risk level of the schemes within the Potential Risk Class (PRC).
18	Ensure and comply with such other matters specified by the Securities and Exchange Board of India (Mutual Funds) Regulations, 1996 read with various amendments and clarifications issued by SEBI from time to time. and SEBI Risk Management Circular dated 27th September 2021

DSP
ASSET MANAGERS

Risk Management - Role of the Executive Risk Management Committee (ERMC)

1	Ensure formulation, implementation, periodic update and approval of various mandatory risk management policies and framework
2	Establishing an organization-wide risk-conscious culture
3	Define, approve, monitor and report breaches in code of conduct to the RMC
4	Annual review of roles and responsibilities of the CRO and CXOs and the Delegation of Power (DoP) w.r.t risk management activities of the management.
5	Review, monitor and ensure adherence to the risk appetite and tolerance limits for risk metrics
6	Approve tolerance limits against each of the risk metric
7	Review and escalate major findings, exceptions, deviations, resolution, strategies to the RMC for any existing risk and emerging risks identified
8	Approve key risk and risk registers proposed by CXOs Capturing: Measurement criteria, measurement tool, monitoring and reporting frequency, reporting of breaches
9	Mechanism for risk monitoring and reporting: early warning signals, monitor mis-selling, review of distributors
10	Systems to detect and prevent security market violation, frauds and malpractices by the AMC
11	Assess and review of the following: Red flags from monitoring of early warning signals, Monthly reporting to CEO, Monthly and Quarterly risk reports submitted by functions, Internal review pertaining to outsourced activities, Testing of internal controls over financial reporting, Governance risk and conflict of interest in investee company, Review Incident and Event reported as per the Operating Event Management Policy including control breaches and mitigating actions for control gaps
12	Review, analyse and escalate internal and external fraudulent incidents to ERMC
13	Ensure Insurance cover is obtained for first-and third-party losses.
14	Review external agency reports on periodic review of verification of efficacy of corporate governance standards and business line compliances, validation of the RMF and assurance over the risk management processes.
15	Assist the AMC and Trustee RMCs and delegate such other responsibilities to the management as may be required in discharging its duties.

Risk Management - Role and KRAs of CEO

1	The CEO shall be responsible for monitoring and managing risks at both AMC and Scheme level.
2	The CEO shall ensure that the outcomes of risk management function are reported to him on a monthly basis
3	The CEO shall define specific roles and responsibilities including KRAs of CXOs regarding risk management
4	The CEO shall define a risk appetite framework for schemes and AMC and place these at the risk committees for approval
5	The CEO shall define appropriate risk metric for respective CXOs, fund manager, etc.
6	The CEO shall define Delegation of Power (DoP) framework for daily risk management, reporting and corrective actions and place it with Board of AMC and Trustees for approval.
7	The CEO shall 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

8	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
9	Review identified fraud incidents along with corrective action plans and report to the risk committee
10	Review risks events and operating events across different functions and approve corrective / recommended actions highlighted by the CIO and other CXOs

Risk Management - Role and KRAs of CRO

1	The CRO shall be responsible for implementation and governance of Risk Management Framework ("RMF") across Asset Management Company ("AMC") and Mutual Fund Schemes
2	The CRO shall be responsible for ensuring all risk related policies are defined, reviewed, and updated periodically and placed at the relevant committee for approval.
3	Aiding ERMC in establishing an organization wide risk conscious culture.
4	Formulate and recommend changes to roles and responsibilities relating to risk management activities and place these at the RMCs for approval.
5	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.
6	Put in place mechanism for reporting to CEO - Including outcomes for risk management function on monthly basis
7	Perform periodic review and update the RMF defined by the AMC and place the same to the Risk Management Committee ("RMC") for approval.
8	Review and suggest changes to the risk appetite and risk metrics for AMC and scheme as defined by the CEO and CXOs
9	Periodically review the Delegation of Power (DoP) covering the following: o Daily risk management o Daily risk reporting o Corrective actions at the level of Fund manager, Heads of Investment Functions and CEO
10	o The CRO shall inform 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.
11	Ensure formulation and implementation of adequate mechanism for – o Aiding CXOs with setup for generating early warning signals and reviewing periodical alerts o Ensure stress testing for investment, credit and liquidity risks basis approved parameters are duly performed and results evaluated by the relevant committee. o Recommend changes in the tolerance limits of risk metric to CEO. o Measurement and review of AMC and scheme specific risks including RCSA and the person responsible to monitor the risks. o Recommend changes in the credit risk policies approved by credit committee o Ensure assessment of liquidity risk at a scheme level and ensure adequate corrective action are taken where required o Ensure assessment and corrective actions for alerts pertaining to asset liability mismatch o Formulation of Fraud Risk Registers and Frauds response plan / strategies o Review Escalations and resolution of incidents as per the Operating Event Management Policy (loss, near miss, fraud etc.) o Ensure review of operations for material outsourced activities at least on an annual basis.
12	Review and report the following to the ERMC and RMC of AMC and Trustee o Risk reports and dashboards capturing deviations to risk thresholds, risk appetite across AMC and Scheme o Results of monitoring of early warning signals by respective functions o Result of stress testing based on defined parameters for investment, credit and liquidity risks, etc.

	○ Internal and external fraud incidents reported / identified by CXOs including evaluation of fraud risk scenarios ○ Incidents identified and reported by the respective departments as per the Operating Event Management Policy ○ Monitor liquidity risk including asset liability mismatch at a scheme and portfolio level vis-à-vis internally approved and defined liquidity model on a monthly basis ○ Major findings and corrective actions prepared by the CXOs ○ Monitor delays in implementation of corrective actions by CXOs ○ Monitor control breaches as a result of periodic RCSA review and mitigating actions put in place by the management and risk function.
13	Ensure insurance cover is maintained based on AMC and Trustee approval for the MF operations and third-party losses
14	Define process to assess the control against each of the identified risk capturing following elements: ○ Measurement tool for each risk ○ Monitoring and reporting frequency ○ Reporting of breaches
15	Identify, assess and estimate emerging risks and their possible impact on AMC and mutual fund schemes and escalate material emerging risk to RMC

Risk Management - Role and KRAs of Head – Investments

1	Daily management of risk and reporting of any breaches as per DOP relating to Investment risk of all schemes(s) such as market Risk, liquidity Risk, credit risk etc. and other scheme specific risks (Compliance Risk, Fraud Risk, etc.)
2	Ensure defining specific responsibility of Fund Managers
3	Ensure adherence to risk appetite framework and maintain risk levels for schemes
4	Calculate the overall risk by taking in to account the weighted average of (i) the risk-o-meter and (ii) the events of defaults. Both (i) and (ii) are to be calculated in terms of a number taking into account the risk-o-meter and events of defaults or early mortality of investments which may inter alia include credit default, change in yield, change in NAV, external shock or unusual redemptions, etc. to quantify the overall risk
5	Escalate the corrective actions taken, if any, to the CEO and the CRO
6	Review and provide recommendations for changes to the Investment and other policies such as credit risk policy, liquidity risk policy and governance risk policy and place it with Board for approval
7	Ensure adherence to the Operating Event Management policy
8	Recommend changes in the investment policies and ensuring they are aligned to the investment objectives as documented in the Scheme Information Document ("SID")
9	Formulate, review and implement a framework for - ○ Updation / modification in the equity or debt investment universe ○ Updation in internal investment limits. ○ Provide relevant information to CRO regarding the risk reports ○ Quantitative risk analysis (using metrics such as VaR, Sharpe Ratio, Treynor Ratio, Information Ratio, etc.) ○ Review portfolio concentration and take necessary actions to make adjustments to the portfolio holding ○ Monitoring risk appetite within the potential risk class of the respective schemes ○ Assessment of the governance risk of the issuer ○ Assessing and monitoring risks of investing in multiple markets ○ Maintenance of all relevant documents and disclosures with regard to the debt and money market instruments before finalizing the deal ○ Ensuring that schemes are managed in line with regulatory requirements
10	Manage and monitor investment risks by reviewing published reports and taking corrective action basis the following – ○ Redemption analysis

	○ Investor concentration analysis ○ Distributor concentration analysis
11	Ensure adherence to the "Stewardship Code" and other regulatory updates prescribed by SEBI for mutual funds
12	Ensure periodic reviews and monitoring the following – ○ Activities performed by fund managers with respect to risks identification, risk management, reporting and corrective actions. ○ Review and approve the changes to the risk appetite within the potential risk class of the respective schemes ○ Exceptions / breaches to the Investment limits and identify and implement corrective actions. ○ Investment risk for new products ○ Implementation of controls around dealing room such as – ▪ non usage of mobile phones ▪ handling of information ○ Ensure adequate due diligence are conducted and documented during inter-scheme transfers
13	Monitor exceptions identified on review of the regular risk management activities
14	Review 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 across all schemes
15	Ensure that fund managers and dealers comply with Code of Conduct as per Schedule V B of Mutual Fund Regulations.

Risk Management - Role and KRAs of Fund Managers

1	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 within approved limits and appropriate risk reporting of any risk related event to respective CXO
2	In respect of schemes managed by them, FMs should ensure adherence to risk appetite framework to maintain appropriate risk level for schemes
3	Recommend reduction/ change in the risk level of the schemes within the Potential Risk Class (PRC) to the CIO
4	The FM shall take corrective action, if required, as per the approved DoP and escalate major risk related event to respective CXO.
5	Ensure adherence of applicable provisions of Mutual Funds Regulations including Code of Conduct per Schedule V B.
6	Suggest / provide inputs on changes required to risk appetite to the Head Investments
7	Report identified risk, risk related events, other operating events and corrective actions plans to the CIO
8	Measure risks in accordance with the approved internal policy and risk metric.
9	Periodic analysis of bulk trades and block deals of large values.
10	Analysis and evaluation of ratings received from multiple credit rating agencies for securities across portfolios and take necessary actions
11	Review 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 across all schemes
12	Manage and monitor investments in schemes by reviewing published – ○ Quantitative risk analysis using metrics such as VaR, Sharpe Ratio, Treynor Ratio, Information Ratio, etc. ○ analysis of concentration limits (counterparty wise, group wise, industry or sector wise, geography wise)
13	Perform due diligence at the time of buying securities through inter-scheme transfers
14	Ensure maintenance of all relevant documents and disclosures with regard to debt and money market instruments before finalizing the deal

DSP
ASSET MANAGERS

Risk Management - Role and KRAs of Head – Sales & Distribution

1	Responsible for the governance of business risks including distribution risks.
2	Provide inputs to CRO to define risk threshold and risk appetite
3	Define and delegate roles to the key personnel within the distribution / sales function for identifying and reporting risks
4	Provide relevant information to CRO regarding the risk reports
5	For the relevant functional risks, identify, analyze and report the following to the CRO and CEO along with recommended action plan for: o Early warning signals o Emerging risks o Major findings o Near miss and loss events o Fraud incidents Ensure escalation of such incidents as per the escalation matrix approved by CRO.
6	Review the risk level for the functional risk is in accordance with the approved risk threshold and risk metric.
7	Ensure adherence with the DoP framework
8	Formulate, review and periodically provide inputs to update the RCSA for key risks and controls; and report outcomes of periodic testing of the RCSA
9	Identify and report operating events and implement corrective actions / recommend action plans for deviations in the controls and present to CRO and CEO
10	Monitor the distribution channels and miss-selling incidents reported such as – o Number of mis-selling incidents o Negative comments in the inspection report relating to distribution o Analysis of the portfolio of investors e.g., nature of investments vis-à-vis risk appetite of investor
11	Exceptions reported by Sales & Marketing basis reviews done for distributors.

Risk Management - Role and KRAs of Head – Integrated Marketing

1	Responsible for the governance of risks pertaining to integrated marketing (Consumer Marketing, Distributor marketing, Digital marketing and Digital product management) function.
2	Provide inputs to CRO to define risk threshold and risk appetite for identified risk areas
3	Provide relevant information to CRO regarding the risk reports
4	For the relevant functional risks, identify, analyze and report the following along with recommended action plan for: o Early warning signals o Emerging risks o Major findings o Loss events and business disruption events o Fraud incidents Ensure escalation of such incidents as per the approved escalation matrix .
5	Review and ensure that the risk level for the function is in accordance with the approved risk threshold and risk metric.
6	Ensure adherence with the DoP framework
7	Formulate, review and periodically provide inputs to update the RCSA for key risks and controls; and report outcomes of periodic testing of the RCSA
8	Identify, report operating events and implement corrective actions / recommend action plans for deviations in the controls

9	Monitor fraud vulnerabilities in the business processes including outsourced process
10	Ensure least system failures affecting business and deliverable of other functions
11	Ensure adherence to the 1. SEBI regulations & circulars 2. Laid down Business Continuity Plan 3. Laid down Cyber-security and Cyber resilience framework 4. Laid down Audit framework
12	Ensure adherence to the SEBI risk management framework
13	Monitor the digital distribution channels and miss-selling incidents reported such as – ○ Number of mis-selling incidents ○ Negative comments in the inspection report relating to distribution

Risk Management - Role and KRAs of Head – Legal & Compliance

1	Responsible for the governance of compliance risks.
2	Formulate and implement compliance and other policies such as prevention of front running, outside business activity, commercial bribes and kickbacks, whistle blowing policy, record retention policy, outsourcing arrangements, etc. in accordance with SEBI risk management framework and approved by the Board of AMC and Trustee
3	Review and suggest changes in the policies and obtain approval from Board of AMC and Trustee
4	Ensure identification and communication of regulatory updates to the respective functions and CXOs and monitor implementation
5	Provide inputs to CRO to define risk threshold and risk appetite of Compliance
6	Define and delegate roles to the key personnel within the compliance function for identifying and reporting risks
7	Provide relevant information to CRO regarding monthly / quarterly risk reporting to the Committees
8	For the relevant functional risks, identify, analyze and report the following to the CRO and CEO along with recommended action plan for: ○ Early warning signals ○ Emerging risks ○ Major findings ○ Near miss and loss events ○ Fraud incidents Ensure escalation of such incidents as per the escalation matrix approved by CRO.
9	Ensure timely and accurate filing of the regulatory returns / filings
10	Review the risk level for the functional risk is in accordance with the approved risk threshold and risk metric
11	Ensure adherence with the DoP framework
12	Formulate, review and periodically provide inputs to update the RCSA for key risks and controls; and report outcomes of periodic testing of the RCSA
13	Identify and report operating events and implement corrective actions / recommend action plans for deviations in the controls to CRO and CEO
14	Ensure timely submission of regulatory reports to the Regulator and Board of AMC and Trustee as prescribed by the SEBI Mutual Funds Regulations.
15	Monitor the following scheme related disclosures - ○ Disclosure of credit (quality of investments made mainly debt based on the credit rating), counterparty, investment and other risks associated with the scheme to the investors ○ Scheme's risk profile is stated in all communications with investors including in the SID and marketing materials

	○ Incorporate any other elements of risk appetite as may be stipulated by AMCs and Trustees in SID
16	Implement process for prevention or detection of possible insider trading at the personnel or portfolio levels
17	Implement process for performing compliance check of AMC's marketing materials (collateral, brochures etc.), website uploads, digital advertising, and performance advertising etc. before its usage.
18	Ensure that roles and responsibilities as per the RMF is disclosed on the AMC website

Risk Management - Role and KRAs of Head – Fund Administration

1	Responsible for the governance of operational risks.
2	Provide inputs to CRO to define risk threshold and risk appetite
3	Define and delegate roles to the key personnel within the operations function for identifying and reporting risks
4	Provide relevant information to CRO regarding the risk reports
5	For the relevant functional risks, identify, analyze and report the following to the CRO and CEO along with recommended action plan for: ○ Early warning signals ○ Emerging risks ○ Major findings ○ Near miss and loss events ○ Fraud incidents Ensure escalation of such incidents as per the escalation matrix approved by CRO.
6	Perform adequate due diligence of outsourced vendors prior to onboarding
7	Ensure periodic assessment of outsourced vendors and assess control function for critical processes in adherence to the laid down organisational outsourcing policy
8	Ensure adequate segregation of duties within the finance function for accounting related activities for scheme and AMC
9	Ensure risk level are in accordance with the approved risk threshold and risk metric.
10	Ensure adherence with the DoP framework
11	Formulate, review and periodically provide inputs to update the RCSA for key risks and controls; and report outcomes of periodic testing of the RCSA
12	Identify, report operating events and implement corrective actions / recommend action plans for deviations in the controls and present to CRO/ CEO
13	Formulate and implement policy for mutual fund accounting and obtain approval from the Board of AMC. Also perform periodic review and suggest changes wherever required.
14	Formulate procedure documents and implement process to perform periodic testing of internal controls over financial reporting of Mutual Fund schemes

Risk Management - Role and KRAs of Head – TA Operations and Client Service

1	Responsible for the governance of operational risks.
2	Provide inputs to CRO to define risk threshold and risk appetite
3	Define and delegate roles to the key personnel within the operations function for identifying and reporting risks
4	Provide relevant information to CRO regarding the risk reports
5	For the relevant functional risks, identify, analyze and report the following to the CRO and CEO along with recommended action plan for: ○ Early warning signals ○ Emerging risks ○ Major findings

	○ Near miss and loss events ○ Fraud incidents Ensure escalation of such incidents as per the escalation matrix approved by CRO.
6	Perform adequate due diligence of outsourced vendors prior to onboarding
7	Ensure periodic assessment of outsourced vendors and assess control function for critical processes in adherence to the laid down organisational outsourcing policy
8	Ensure risk level are in accordance with the approved risk threshold and risk metric.
9	Ensure adherence with the DoP framework
10	Formulate, review and periodically provide inputs to update the RCSA for key risks and controls; and report outcomes of periodic testing of the RCSA
11	Identify, report operating events and implement corrective actions / recommend action plans for deviations in the controls and present to CRO/ CEO

Risk Management - Role and KRAs of Head – Human Resources

1	Responsible for the governance of Human Resource risks
2	Formulate and implement Human Resources and remuneration policy and obtain approval from the Board of AMC
3	Review and suggest changes in the policies and obtain approval from Board of AMC
4	Provide inputs to CRO to define risk threshold and risk appetite
5	Define and delegate roles to the key personnel within the human resource function for identifying and reporting risks
6	Provide relevant information to CRO regarding the risk reports
7	For the relevant functional risks, identify, analyze and report the following to the CRO and CEO along with recommended action plan for: ○ Early warning signals ○ Emerging risks ○ Major findings ○ Near miss and loss events ○ Fraud incidents Ensure escalation of such incidents as per the escalation matrix approved by CRO.
8	Review the risk level for the functional risk is in accordance with the approved risk threshold and risk metric.
9	Ensure adherence with the DoP framework
10	Formulate, review and periodically provide inputs to update the RCSA for key risks and controls; and report outcomes of periodic testing of the RCSA
11	Identify, report operating events and implement corrective actions / recommend action plans for deviations in the controls and present to CRO/ CEO
12	Ensure a well-defined succession planning process for KMP and other key positions in the AMC
13	Ensure that risk related KRAs are defined for all executives up to two levels below CEO

DSP
ASSET MANAGERS

Risk Management - Role and KRAs of Chief Technology Officer

1	Responsible for the governance of Technology, Information Security and Cyber risks
2	Provide inputs to CRO to define risk threshold and risk appetite
3	Provide relevant information to CRO regarding the risk reports
4	For the relevant functional risks, identify, analyze and report the following to the CRO and CEO along with recommended action plan for: o Early warning signals o Emerging risks o Major findings o loss events and business disruptions o Fraud incidents Ensure escalation of such incidents as per the escalation matrix approved by CRO.
5	Review the risk level for the functional risk is in accordance with the approved risk threshold and risk metric.
6	Ensure adherence with the DoP framework
7	Formulate, review and periodically provide inputs to update the RCSA for key risks and controls; and report outcomes of periodic testing of the RCSA
8	Identify, report operating events and implement corrective actions / recommend action plans for deviations in the controls and present to CRO/ CEO
9	Monitor fraud vulnerabilities in the business processes including outsourced process
10	Ensure least system failures affecting business and deliverable of other functions
11	Frame and ensure adherence to the Business Continuity Plans and the required systems are in place and updated periodically
12	Frame a cyber-security and cyber resilience framework and audit framework encompassing systems and processes for Mutual Funds/AMCs and suggest timely changes to ensure effectiveness of the framework
13	Ensure adherence to SEBI circulars, SEBI/HO/IMD/DF2/CIR/P/2019/12, SEBI/HO/IMD/DF2/CIR/P/2019/57, SEBI/HO/IMD/DF2/CIR/P/2019/58 dated January 10, 2019 and April 11, 2019, and all subsequent amendments
14	Ensure implementation of an integrated investment management system across front office, mid office and back office

Risk Management - Role and KRAs of Other Function heads

1	The CXOs shall be responsible for the governance of the respective risk types
2	In respect of respective risk type, CXO should 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
3	In respect of respective risk type, CXO should ensure defining specific responsibility regarding risk management of key personnel reporting to them
4	Maintaining risk level as per the risk metric
5	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.
6	The CXO shall escalate to CEO and the CRO any major findings reported by respective risk management function
7	Identify, report operating events and implement corrective actions / recommend action plans for deviations in the controls and present to CRO/ CEO

DSP
ASSET MANAGERS

Role and KRAs of Chief Financial Officer:

1	Responsible to oversee the governance framework for financial accounting and reporting risks within the organization.
2	Ensure accurate and timely financial reporting in accordance with regulatory standards and internal policies.
3	Formulate and implement policies for mutual fund accounting in alignment with regulatory requirements.
4	Perform periodic reviews of accounting policies, suggest necessary changes, and obtain approval from the Board of AMC.
5	Provide inputs to the CRO to define risk thresholds and risk appetite for the organization.
6	Define, delegate, and oversee roles within the finance and accounting function for identifying and reporting financial risks.
7	Regularly provide relevant financial risk information to the CRO regarding risk reports.
8	Identify, analyze, and report critical financial risks, including: Early warning signals Emerging risks Major findings Near-miss and loss events Fraud incidents
9	Ensure that any financial incidents or deviations are escalated according to the escalation matrix approved by the CRO.
10	Safeguard against fraudulent activities and ensure that accounting-related activities are managed in a structured, compliant manner for both the schemes and the AMC.
11	Review and ensure that the risk level for the function is in accordance with the approved risk threshold and risk metric
12	Monitor the effectiveness of financial risk management strategies and recommend adjustments as needed to stay within acceptable risk levels.
13	Formulate, review and periodically provide inputs to update the RCSA for key risks and controls; and report outcomes of periodic testing of the RCSA
14	Ensure adherence with the DoP framework
15	Identify, report operating events and implement corrective actions / recommend action plans for deviations in the controls
16	Ensure that all financial and risk management practices align with SEBI risk management frameworks and comply with related regulations
17	Formulate and implement procedural documents to establish regular testing of internal controls over financial reporting for both AMC and Trust Company books of accounts.
18	Ensure these controls are in place and updated periodically to prevent errors, fraud, and regulatory non-compliance.

Role and KRAs of Chief Information Security Officer:

1	Responsible to develop, implement, and monitor strategic and comprehensive enterprise Information Security and Cyber risk management program
2	Frame and manage the cybersecurity and cyber resilience framework, ensuring systems and processes are continually updated for Mutual Funds/AMCs.
3	To review and disseminate the Information security policies by ensuring that they are current and reflecting the requirement of DSP Asset Managers and government regulators
4	Provide inputs to CRO to define risk threshold and risk appetite Provide relevant information to CRO regarding the risk reports
5	For the relevant functional risks, identify, analyze and report the following to the CRO and CEO along with recommended action plan for:

	O Early warning signals O Emerging risks O Major findings O Cyber security events / Cyber Frauds etc.
6	Ensure escalation of such incidents as per the escalation matrix approved by CRO. Partner with business stakeholders across the company to raise awareness around Information security
7	Ensure adherence to the 1. SEBI regulations & circulars 2. Laid down Business Continuity Plan 3. Laid down Cyber-security and Cyber resilience framework 4. Laid down Audit framework
8	Review the risk level for the functional risk is in accordance with the approved risk threshold and risk metric.
9	Ensure adherence with the DoP framework
10	Formulate, review and periodically provide inputs to update the RCSA for key risks and controls; and report outcomes of periodic testing of the RCSA Identify, report operating events and implement corrective actions / recommend action plans for deviations in the controls and present to CRO/ CEO
11	Frame and ensure adherence to the Business Continuity Plans and the required systems are in place and updated periodically
12	Frame a cyber-security and cyber resilience framework and audit framework encompassing systems and processes for Mutual Funds/AMCs and suggest timely changes to ensure effectiveness of the framework
13	Ensure adherence to SEBI circulars, SEBI/HO/IMD/DF2/CIR/P/2019/12,SEBI/HO/IMD/DF2/CIR/P/2019/57, SEBI/HO/IMD/DF2/CIR/P/2019/58 dated January 10,2019 and April 11, 2019, and all subsequent amendments

Role of internal auditor: There will be an internal auditor appointed for audit of the RMF. The personnel undertaking the audit will have relevant expertise in the domain of risk management necessary for both the AMC level and the scheme level audit.

The internal auditor will audit both the scheme level and AMC level risks. The internal auditor will 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. For the processes being audited by the internal auditor, a non-compliance rate will be computed. The non-compliance rate may be computed based on sampling out of the total number of processes being audited. The internal auditor will submit the internal audit report to the audit committee of the AMC and the Board of AMC representing the non-compliance rate as audited in the books of accounts of the AMC and its schemes. While submitting to the audit committee, the non-compliance 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. Further, this number shall be compared in subsequent internal audits to analyse the improvement in minimizing the non-compliance level at the AMC. This shall reflect the degree of rectification of non-compliance 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

II. Identification of Risks

These key risks are divided into two broad categories.

- **Scheme specific risks:** The scheme specific risks are the risks majorly associated with the core activities of investment and portfolio management
- **AMC specific risks**: The AMC specific risks are the risks associated with the functioning of the mutual fund business by the AMC

The **Scheme specific risks** are divided into the following categories

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

- **Credit risk**: 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

- **Liquidity risk:** 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

- **Governance risk:** 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

- **Compliance Risk:** Failure by the AMC to meet its regulatory obligations or manage changes in legal statutory and regulatory requirements for its investment management activity at a scheme level which may result in investigations, fines, financial forfeiture, or regulatory sanctions and material loss to investors and the organization.

The **AMC specific risks** are divided into the following categories:

- **Operational Risk**: 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

- **Compliance Risk**: 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

- **Technology, Information Security and Cyber Risk**: 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

- **Reputation and Conduct Risks**: 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

- **Outsourcing Risk:** 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

- **Sales and Distribution Risk**: 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

- **Financial Reporting Risk:** Absence of internal control over financial reporting with regard to the mutual fund schemes, may pose the risks
    - Improper maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of assets
    - 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
    - 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

- **Legal & Tax Risks:** Legal & Tax risk is the risk of loss to an institution which is primarily caused by:
    - A defective transaction
    - 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).
    - Failing to take appropriate measures to protect assets (for example, intellectual property) owned by the institution.
    - Change in law
    - Misinterpretation of statutes and regulations.
    - Failure to collect or pay appropriate taxes, or submit required returns or information

- **Talent Risk:** Talent risk is the risk of not having the right people in place at the right time to drive current and future business growth

Risk Appetite Framework

DSP Asset Managers has developed a 4-point risk rating scale to quantify impact that an occurrence of each of the risks would have on DSP's ability to achieve its strategic priorities after considering existing controls / risk management activities.

The impact assessment considers financial, reputational, operational, legal and investor impact of the occurrence of the risk.

The probability of the happening of each of the above risks considers the control environment and automation, external factors or dependencies such as market infrastructure, outsourced activities, etc. and available historical risk data.

Based on the impact assessment of the risk and considering the control environment, a formalized risk appetite statement with a rationale for the same is documented for each of the key functions/risk types, incorporating key risk scenarios that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives, sources of risks and areas impacted due to the event. The risk appetite statement aims to provide an objective articulation of the aggregate level and types of risk that DSP is willing to accept, or to avoid achieving its business objectives within the regulatory requirements. It includes qualitative statements as well as quantitative measures.

The definitions for the risk rating scale are given below:

Scale	Risk Appetite	Definition
1	**Very low**	DSP has **Very limited** appetite for the risk and so takes every reasonable action to avoid unfavourable outcomes No trade-off between business returns vs. cost considerations, and design business processes and controls with an emphasis on avoiding risk
2	**Low**	DSP has **Limited appetite** for the risk, but accepts that there may be some (very limited) unfavourable outcomes Some deliberate trade-offs between business returns / cost to take on some risk We may differentiate between the types of unfavourable outcomes, e.g., we risk accept some activities but focus our efforts and the design of controls to avoid or mitigate the more material
3	**Medium**	DSP has **Greater appetite** for the risk and either accepts and/or expects some more frequent, or more severe, unfavourable outcomes Deliberate trade-offs between business returns vs. cost considerations to assume some risk Accept activities not because we want to but because we have to, since the risk is intrinsic to asset management or to the environment in which we operate, so we can influence but ultimately not completely control the risk
4	**High**	**Significant appetite** for the risk and routinely expects and accept potentially severe unfavourable outcomes Trade-offs between business strategy / cost considerations to take on riskier activities Accept many activities, including those with higher residual risk for reasons such as expedited execution Embark on activities before introducing risk mitigants, substantive or tested controls, and introduce risk mitigants or controls at a later date

		May wait to see the impact of unfavourable outcomes and remediation costs before introducing risk mitigants or substantive controls

For each risk type, in addition to the key risk scenarios, DSP has also documented the emerging or new risks due to new business lines, new products, statutory changes, changes in external environment or market infrastructure, etc

For each scheme managed by DSP, a risk appetite has been defined. The scheme risk appetite considers the asset class and investment strategy adopted by the scheme

III. Measurement and Management of Risks

DSP has defined risk metrics for measurement of various scheme specific risks, including investment risk, credit risk, liquidity risk).

Apart from the scheme risk metrics, risk metrics have also been defined for each of the key AMC specific risks.

Risk metrics are measurable with defined risk thresholds. The risk thresholds are based on the risk appetite and consider control environment as well as other aspects such as historical experience, peer benchmarking, regulatory requirements/ guidelines etc. Each metric has a determined frequency of monitoring and an escalation process in the event of a breach of the threshold. Appropriate remedial or mitigating actions will be taken in the event a risk metric exceeds the defined threshold.

Delegation of Power and Escalation Process

DSP has defined a Delegation of Power framework covering daily risk management, daily risk reporting and corrective actions at various levels of management, with the following roles:

- **Responsible:** Always the first step and indicates the beginning (initiation) of activity
- **Accountable:** Provides authority for taking appropriate action or decision on the outcome of the activities
- **Approval / Corrective action in case of breach beyond the threshold approved under RMF:** Provides inputs to authority relating to identified risks and deviations and approves Corrective action or breaches beyond the threshold approved under RMF
- **Informed:** Presentation of Information to the authority for their attention and action

Risk and Control Self-Assessment (RCSA)

A Risk and Control Self-Assessment (RCSA) is the process for identifying and assessing risk within a business and evaluating the effectiveness of the controls that such business has in place to mitigate/manage these risks

RCSA Objectives: RCSA is a tool to enable DSP Asset Managers to:

- Proactively identify key risks (existing and emerging)
- Assess associated controls to determine level of mitigation and preparedness
- Strengthen controls and lower the risk of operating events

- Document actions for any control weaknesses and prioritise and manage those risks
- Facilitate management of risks effectively and efficiently by senior management within the businesses
- Prioritize and allocate resources to focus on higher risk areas
- Raise awareness of the risks across the organization
- Identify and assess the operational and compliance risks, including conduct risks
- Identify and assess the controls in place to mitigate those risk
- Document actions for any control weaknesses and prioritise those actions according to the risk they pose to AMC

Principles:

- RCSAs to be reviewed once every year. However, in case there is a change **in process**/new process/ multiple operating events, Enterprise Risk Management team can guide respective functions to do ad-hoc RCSAs.
- DSP Asset Managers has developed a 4-point risk rating scale to quantify inherent and residual risk
- Functional CXOs will identify critical areas / processes that should conduct RCSA. The functional CXO should consider the following for the RCSAs that he/she owns or facilitates
    - Recent operating events and what they reveal about the risks and controls as documented in the RCSA
    - External events (control failings at other competitor firms) and what they reveal about the risks and controls as documented in the RCSA
    - Emerging risks and early warning indicators, including adverse trends observed in any of the risk metrics and operating events
    - Significant changes (e.g., organizational, regulatory, new products/instruments, growth, etc.) impacting the business
    - Other High or Medium actions (open or recently closed) tagged to the business including, risk and control issues
    - Additionally, Risk Management Committee may also advise specific areas that should conduct RCSAs
- Functional CXOs will sign-off the RCSAs
- The 1st line of defense (business areas) will assess their Inherent and Residual risk and evaluate the effectiveness of controls in place to mitigate risks in identified critical areas / day-to-day core processes
- The 2nd line of defense (CRO) will review the RCSAs and provide comments.
- RCSA results will be reviewed by the CRO & second line of defense and presented to the Risk Management Committee. Necessary corrective actions will be taken by the functions to address any short comings

The RCSAs will be reviewed in the event of material claims or litigations from customers or incidents, material findings from internal or external audits, adverse media attention impacting reputation risk, adverse observations from the regulator(s), key risk indicator breaches, new regulatory requirements, sector-relevant developments or incidents

Policy reviews: Periodic review of policy frameworks will be done to ensure that all 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

IV. Reporting of Risks and Related Information

Each CXO will be responsible for reporting the risk metrics for their function on a timely basis to the CRO and the risk management team. This bottom-up reporting process ensures that the risk management function can perform timely, meaningful, and independent analysis of such information.

The risk metrics will be reported based on the pre-defined frequency.

Further all the employees and CXOs have to ensure adherence to the Operating Event Management Policy which has been adopted by DSP with the following objective. The Operating Event Management Policy sets out roles, responsibilities, and requirements to facilitate timely identification, reporting and management of operational risk events. This is critical to minimize any financial, operational, legal, or reputational impact to DSP Asset Managers Pvt. Ltd. (DSP) and its clients.

The process of capturing and assessment of information regarding the circumstances of an operating event provides DSP with the opportunity to reflect upon end-to-end processes, systems and controls and enhance them as required. DSP can learn from operating events to improve and fortify the processes and controls.

The outcomes of the risk management function will be mandatorily reported to the CEO and senior management personnel on a monthly basis and to the RMC 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.

The risk reports will incorporate the risk metrics for all schemes for AMC specific risks and will be consolidated across the departments and the AMC level. They will also incorporate the rectification index as calculated in the internal audit report for both the AMC and the scheme level. Risk reports will contain information on impact assessment of the risk as well as measures and corrective actions taken by the management to control and mitigate the relevant risks. The risk reports will capture trends in evolution of the risk metrics to flag off early warnings and adverse trends.

In addition, the CRO and risk management function may also report any significant emerging risk issues that are not covered in the scheme and AMC risk metrics in the risk reports.

Version Control

Date	***Version***	***Rationale***	***Team ownership***
April 1, 2023	*v1.0*	*Demerger*	*ERM Team*
April 26, 2024	*V1.1*	*Annual policy review*	*ERM Team*
April 25,2025	*V1.2*	*Annual policy review*	*ERM Team*
Oct 29,2025	*V1.3*	*Inclusion of provision for subsidiary companies*	*ERM Team*