भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

CIRCULAR

SEBI/HO/IMD/DF2/CIR/P/2019/57

April 11, 2019

All Mutual Funds/
Asset Management Companies (AMCs)/
Trustee Companies/ Boards of Trustees of Mutual Funds/
Registrar and Transfer Agents/
Association of Mutual Funds in India (AMFI)

Dear Sir/Madam,

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

1. Requirement of system audit for mutual funds was introduced vide SEBI Circular SEBI/IMD/CIR No.9/176988/2009 dated September 16, 2009.

2. Considering the importance of systems audit in technology driven asset management activity and to enhance and standardize the systems audit, revised guidelines in this regard are placed at **Annexure 1**. These guidelines are indicative and not exhaustive in nature. On the date of issuance of this circular, SEBI Circular SEBI/IMD/CIR No.9/176988/2009 dated September 16, 2009 shall stand rescinded.

3. The aforementioned audit should be encompassing audit of systems and processes, inter alia, related to examination of integration of front office system with the back office system, fund accounting system for calculation of net asset values, financial accounting and reporting system for the AMC, Unit-holder administration and servicing systems for customer service, funds flow process, system processes for meeting regulatory requirements, prudential investment limits and access rights to systems interface.

4. Mutual Funds / AMCs are advised to conduct systems audit on an annual basis by an independent CISA / CISM qualified or equivalent auditor to check compliance of the provisions of this circular.

5. Mutual Funds / AMCs are further advised to take necessary steps to put in place systems for implementation of this circular. The exception report as per **Annexure 2** should be placed before the Technology Committee for review. The Technology Committee after review shall place the same before the AMC & Trustee Board. Thereafter, exception observation report along with trustee comments starting from the financial year April 2019 – March 2020 should be communicated to SEBI within six months of the respective financial year. Further, System Audit Reports shall be made available for inspection.

6. This circular is issued in exercise of powers conferred under Section 11 (1) of the Securities and Exchange Board of India Act, 1992, read with the provisions of Regulation 77 of SEBI (Mutual Funds) Regulations, 1996, to protect the interests of investors in securities and to promote the development of, and to regulate the securities market.

Yours faithfully,

Jyoti Sharma
General Manager
Investment Management Department
Email: jyotis@sebi.gov.in

Annexure -1

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				
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 vide SEBI circular SEBI/HO/IMD/DF2/CIR/P/2019/12 dated January 10, 2019 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 in the event entire approved procedures cannot 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**	**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?

	(DR)		- 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) & DISASTER RECOVERY (DR)**	**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 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 2

Exception (Observation) Reporting Format

Note: Mutual Funds are expected to submit following information with regards to exceptions observed in the System Audit, including open observations from previous audit report.

Name of the Mutual Fund: _____

Systems Audit Report Date: _____

Table 1:

High/ Medium risk exceptions observed in the System Audit, including open observations from previous audit report

S No.	Audit Objective Checklist Question Number	Audit Objective Heading	Department Name	Description of Observation	Risk Rating	Audited By	Auditor's Recommendation	Whether similar issue was observed in any of the previous 2 audits	Management Comment with target date	Trustee Comment

Description of relevant Table heads

1. **S No. –** This indicates the serial number of the observation.
2. **Audit Objective Checklist Question Number –** This indicates question number in the guideline audit checklist
3. **Audit Objective Heading –** This indicates heading in the guideline audit checklist
4. **Department Name –** name of auditee department to which the observation pertains to e.g. PMS, R&TA, IT, Admin etc.
5. **Description of Observation –** Description of the observation in sufficient detail
6. **Risk Rating –** Observation's rating based on its impact and severity to reflect risk exposure.

Rating	Description
HIGH	High rating represents weakness in control with respect to threat(s) that is/are sufficiently capable and impacts asset(s) leading to regulatory noncompliance, significant financial, operational and reputational loss. These observations need to be addressed with utmost priority.
MEDIUM	Medium rating represents weakness in control with respect to threat(s) that is/are capable and impacts asset(s) leading to exposure in terms of financial, operational and reputational loss. These should be addressed reasonably promptly.
LOW	Low rating represents a weaknesses in control, which in combination with other weakness can develop into an exposure. Suggested improvements for situations not immediately/directly affecting controls.

7. **Audit By –** Name of the firm/ company performing the system audit
8. **Auditor's Recommendation** – A detailed recommendation by auditor for correction of the observation and/ or implementation of the corrective actions.
9. **Whether similar issue was observed in any of the previous 2 audits** – Yes/ No if similar issue was observed in previous two audit reports.
10. **Management Comment with target date –** Management action plan/taken to address the observation and/ or implementation of auditor's recommendation with target date to address/implement.
11. **Trustee Comment**– Trustee comments with respect to management action plan/taken to address the observation and/ or implementation of auditor's recommendation with target date to address/implement

Table 2:

Low risk observations in current audit which were observed in previous two System audit reports:

S No.	Audit Objective Checklist Question Number	Audit Objective Heading	Description of Observation	Risk Rating	Management Comment with target date	Trustee Comment
				Low		

Description of relevant Table heads

1. **S No. –** This indicates the serial number of the observation.
2. **Audit Objective Checklist Question Number –** This indicates question number in the guideline audit checklist
3. **Audit Objective Heading –** This indicates heading in the guideline audit checklist
4. **Description of Observation –** Description of the observation in sufficient detail
5. **Risk Rating –** Observation's rating based on its impact and severity to reflect risk exposure.
6. **Management Comment with target date –** Management action plan/taken to address the observation and/ or implementation of auditor's recommendation with target date to address/implement.
7. **Trustee Comment**– Trustee comments with respect to management action plan/taken to address the observation and/ or implementation of auditor's recommendation with target date to address/implement

Table 3:

Follow on Audit for Open Items reported in Table 1 and Table 2 of Previous System Audit Report

S No.	Audited By	Department Name	Description of Observation	Risk Rating	Recommendation as per previous audit report	Reason for delay in implementation/ compliance	Observation Status as per current auditor	Management Comment with revised [Target] Closure Date	Trustee Comment

Description of relevant Table heads

1. **S No.** – Serial number
2. **Audited By –** Name of the firm that performed audit
3. **Department Name –** name of auditee department to which the observation pertains to e.g. PMS, R&TA, IT, Admin etc.
4. **Description of Observation –**Description as per previous System Audit report
5. **Risk Rating of Observation –** Risk rating as per previous System Audit report
6. **Previous Auditor's Recommendation** –Recommendation as per previous System Audit report
7. **Reason for delay in implementation / compliance –** Details of reason for delay in addressing the observation/ implementation of corrective action.
8. **Observation Status per current auditor –** Status of observation in reference to recommendation and management action plan mentioned in the previous system audit report.
9. **Revised [Target] Closure date with Management Comment –** Revised closure date or target closure date for the observation. Management comment is necessary if observation status is not closed as per current auditor.
10. **Trustee Comment–** Trustee comments with respect to revised closure date or target closure date for the observation.