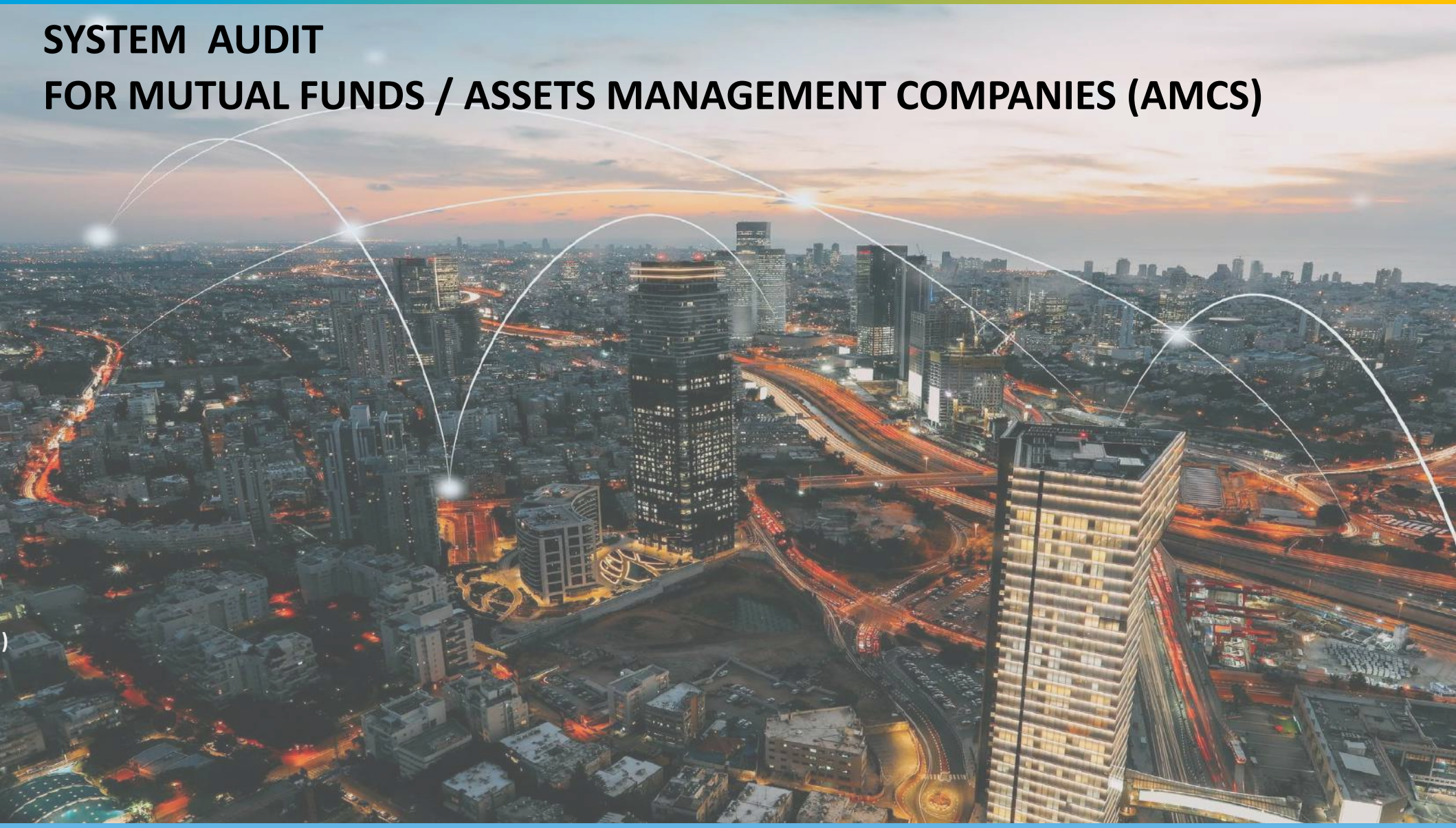
SYSTEM AUDIT
FOR MUTUAL FUNDS / ASSETS MANAGEMENT COMPANIES (AMCS)



ShineWing INDIA

Process, Risk and Technology Advisory

SYSTEM AUDIT

For Mutual Funds / Assets Management Companies (AMCs)

Background

The 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.

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

Mutual Funds / AMCs are further advised to take necessary steps for the exception report. The exception report should be placed for review to the Technology Committee before it placed to the AMC & Trustee Board. Thereafter, exception observation report along with trustee's 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.

The 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

Key Domains of the SEBI Circulars

1. Annexure - 1

- Process of checking the Mutual Funds /AMC's IT Environment based on IT setup & Usage and application systems.

2. System Audit Program Checklist

- Checklist ensures IT Governance , Information Security ,Access change & Incident Management, Backup & Recovery, Job Processing, Business continuity planning, Disaster Recovery& Business controls.

3. Annexure - 2

- The format for exception (observation) reporting includes 3 tables.
- Table 1 for level of Risk observed in system audit from previous audit report
- Table 2 for low level risk observed in previous two audits along with current audit.
- Table 3 for follow on open items on previous system audit report.

SYSTEM AUDIT FRAMEWORK
For Mutual Funds / Assets Management Companies (AMCs)

How can We help?

Perform Current state assessment/ Gap Assessment	Using our inherent industry knowledge and ability to look at risks holistically, we can assist you in assessing the organizations current IT framework vis-à-vis requirements of SEBI mandated Information Technology framework. Our assessment program will also enable benchmarking the organizations measures to identify, protect, detect, respond, and recover from information security and cyber risks and threats to global frameworks.
Development of risk and controls framework to meet requirements	
Conducting training and awareness for employees and vendors	We can help you build your IT security and cybersecurity awareness and training program to enhance the risk culture in your organization.
Post assessment remediation assistance	Advising on remediation plans and program managing the actions to achieve the desired state of IT framework.

Key Performance Indicators

- Improved cost-efficiency of IT processes (costs vs. deliverables)
- Increased number of IT action plans for process improvement initiatives
- Increased utilization of IT infrastructure
- Increased satisfaction of stakeholders (survey and number of complaints)
- Improved staff productivity (number of deliverables) and morale (survey)

1. ANNEXURE - 1
For Mutual Funds / Assets Management Companies (AMCs)

Background

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. It cover the format for IT Environment : Organization details, IT setup & usage and application systems.

(Circular no. SEBI/HO/IMD/DF2/CIR/P/2019/57, dated April,11,2019)

Approach

Our approach & process of checking the Mutual Funds /AMC's IT Environment will be based on understanding and system scoping based on following:-

Understand Organizational Details

- Includes name of the organization & address.
- Organization business
- Understand role of IT and system usage and complexity
- IT organization structure -Size of IT Team (if Employees),Size of IT Team (if Vendors).

IT setup & usage

- Application , it corresponding OS and DB
- Data center and DR site (location, owned/ outsourced) including cloud infrastructre.
- Network Diagram (schematic) with WAN connectivity.
- Network/ Security Systems: (Please specify Version/make/model)which includes Routers, Switches, Proxy Servers, Firewall, Intrusions Detection & prevention Systems, remote access servers, remote access servers, data leakage prevention(specify network and/ or host), privileged identity management.
- Endpoint devices including Operating systems primarily used in workstations.

Application system

- This includes various systems and their interfaces
- E.g.- Back & Front office System, Email, Intranet, File Server, Finance & Accounting System.

2. SYSTEM AUDIT PROGRAM CHECKLIST
For Mutual Funds / Assets Management Companies (AMCs)

Background

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. A quality system auditor closely guards the checklist he uses and can adapt the list to ensure it applies to your business.
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.
(Circular no. SEBI/HO/IMD/DF2/CIR/P/2019/57, dated April,11,2019)

Scope of Audit shall include assessments of the following areas :-

- Information Technology Governance
- Access, Change & Incident Management
- IT backup plan
- Business Continuity Planning (BCP) & Disaster recovery (DR)
- Business Controls on system

Information Technology Governance

IT Governance Framework	IT governance focuses the enterprise goals, strategic initiatives, the use of technology to enhance business and on the availability of sufficient resources and capabilities to keep up with the business demands .
IT Strategy Committee	IT Strategy Committee exists with representations from Board of Directors (BOD), senior IT and business management and reporting to the BOD. IT Strategy Committee meet at least twice in a year.
IT Risk Management	Organization has a defined IT risk management framework covering amongst others process and responsibilities of risk assessment, management and monitoring.
IT Organization Structure	Organization structure must exists with defined authorities, reporting lines and responsibilities related to IT governance including CIO/CTO, CISO and heads of IT team managing operations and applications.
IT Policies and Procedures	IT Strategy & policy documents are approved. & ensured by Mgt. IT Policy should be implemented to operational level involving IT strategy, value delivery, risk management and IT resource management.

2. SYSTEM AUDIT PROGRAM CHECKLIST
For Mutual Funds / Assets Management Companies (AMCs)

INFORMATION SECURITY

Information Security function	Information security function exists distinct from IT function with dedicated responsibility of defining and monitoring implementation of information security policies and controls.
Human Resource Controls	Policies and procedures are implemented to address HR controls as part of information security, hiring policies defined in line with IT operation., background check procedures to be performed for all new joiners
Information Security policy	Security policies are defined, documented and approved by the BOD. Information security framework ensures security requirements are in-built into key IT architecture, operations and other non-IT aspects.
Information Security Risk Management	Defined process should exists and followed for Information security risk management on an annual basis. Risk assessment performed for new functions, processes, teams and locations.
Cyber Security	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.
Information Privacy	Procedures has been defined in line with applicable regulations with respect to privacy notice, choice & consent, access to data, security control for private data.
Information Security Awareness	Information security and cybersecurity processes should be communicated to employees, contractors, third parties and trainings must be conducted as a part of induction as well as periodic trainings.
Third Party Security	Vendor management framework includes processes to be followed for vendor due diligence, selection, risk assessment, onboarding, contracting and monitoring.
Information Security Compliance	Information system review reports, findings and action plans must be reported to IT/ IS risk committees, IT Strategy Committee of BOD as appropriate.

2. SYSTEM AUDIT PROGRAM CHECKLIST
For Mutual Funds / Assets Management Companies (AMCs)

ACCESS MANAGEMENT

Access Review and Monitoring	Control mechanisms such as periodic reconciliation of user lists with HR lists, deactivation of users with no logins for a defined timeframe, etc. has to be deployed to ensure any unauthorized access is timely terminated
Segregation of Duties (SOD)	SOD matrix should describe key roles within the systems and conflicting rights. Access approvals, creations and modifications are performed based on approved SOD matrix.
Physical Security	Physical security mechanisms must be deployed including guarding entrance, usage of access control system, door alarms, turnstiles, biometric access, etc. Environmental security devices should be maintained at regular intervals.
Access Policies and procedures Access	Policies and procedures must exist for managing access to applications and infrastructure (including network, operating systems and database) and must be approved by relevant authority. Risk mitigation measures must be implemented.
Access Administration	Role-based and least privilege access mechanisms must be in-built into systems to enable authorized access as per job roles.
Privileged access	Access rights for privileged users and logs of privileged users must be stored, monitored and reviewed on a periodic basis

CHANGE MANAGEMENT

Change Administration	Changes to applications and infrastructure (networks, operating systems and databases), including requests to third party service providers must be approved and authorized by both authorized IT and business management personnel, as per defined authorization matrix.
Environments and version controls	Organization must implemented a change management versioning tool to maintain audit trails for all types of changes including applications, databases, operating systems and networks.
Segregation of Duties (SOD)	Implemented changes must be reviewed on a periodic basis and if any inappropriate or unauthorized activities are investigated then communication to respective individuals must be done.

2. SYSTEM AUDIT PROGRAM CHECKLIST
For Mutual Funds / Assets Management Companies (AMCs)

INCIDENT MANAGEMENT

Incident Management Policies and Procedures	Incident management policy and procedures must define processes to be followed for incidents related to all systems including applications and infrastructure capturing the version history and approval history.
Incident Resolution	Root cause analysis must be performed and resolution provided against each incident must be documented against the ticket logged. Recurring incidents should be identified and logged as problems.
Service Level Agreements (SLAs)	SLA monitoring reports must be generated and sent to senior management on periodic basis to take relevant actions.
Security Incident Management	Management must have a defined and documented procedures for identifying security related incidents by monitoring logs generated by various IT assets and must be reported to SEBI within stipulated timelines.

BACKUP & RECOVERY

Backup Storage	Backup tapes must be stored at a authorized onsite in a secure fireproof storage. Backup tapes must be sent for offsite storage on a periodic basis which must be monitored periodically.
Backup Administration	Procedures should be in place to ensure back-ups are taken in accordance with the defined back-up strategy and the usability of back-ups is regularly verified.
Restoration	Request based restorations are performed only after obtaining approvals from business head and restoration testing must be performed on a periodic basis and issues, if any must be resolved.

JOB PROCESSING

Job Processing	Automated jobs must be processed as per the approved policies and frequency [e.g., daily, weekly, etc.] and configured via automated tool which restricted to authorized personnel only.

2. SYSTEM AUDIT PROGRAM CHECKLIST
For Mutual Funds / Assets Management Companies (AMCs)

BUSINESS CONTINUITY PLANNING (BCP) & DISASTER RECOVERY

- BCP Organization
- BCP Plan
- BCP Methodology and Plan
- BCP/ DR Communication and training
- BCP/ DR testing
- DR Plan

The BCP may have the following salient features

1. The organization must have 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.
2. Risk Assessment must be conducted for all critical processes identified in the BIA including identification of risks and threats and their impact, probability and priority.
3. 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.
4. BCP plan must be communicated to all users internal as well as external with detailed description of roles, responsibilities and dependencies.
5. d BCP/ DR plan should be 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.
6. DR plan must be in documented format which must includes recovery procedures to be followed in the event of disasters. The organization must implement procedures for maintaining the DR readiness and support infrastructure to be relied upon in the event of a disaster.

BUSINESS CONTROLS

- Master Controls
- Front Office and Back Office Operations
- Investor Servicing
- Risk Management
- Reporting
- Custody of mutual fund scheme assets

1. Access to create/ update/ delete on any master data (Customer/ Scheme/ Securities/ Broker/ Subscriptions/ Redemptions etc.) must be restricted to the authorized individuals.
2. Controls over data integrity, appropriate SOD must be maintained between front office and back office system.
3. Access to create/ update/ delete any master data (Customer/ Scheme/ Securities/ Broker/ Subscriptions/ Redemptions etc.) must be restricted to the authorized individuals.
4. System must monitors adherence to guidelines specified in the Ninth Schedule of the Mutual Fund Regulations with respect to accounting policies.
5. Organization must implement reasonable controls over report generation with respect to accuracy and completeness.
6. System must monitors adherence to controls related to significant accounting and valuation policies along with compliance of SEBI guidelines and PMLA guidelines.

2. ANNEXURE - 2
For Mutual Funds / Assets Management Companies (AMCs)

Background

Annexure 2 has the format for Exception (Observation) Reporting Format. Mutual Funds are expected to submit following information with regards to exceptions observed in the System Audit, including open observations from previous audit report. 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.

(Circular no. SEBI/HO/IMD/DF2/CIR/P/2019/57, dated April,11,2019)

Annexure – 2 includes 3 Tables:-

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

Risk Rating

- **High rating** represents impact on assets leading to non compliance, significant financial, operational & reputational loss and it must be addressed with utmost priority.
- **Medium rating** represents impacts on asset(s) leading to exposure in terms of financial, operational and reputational loss and must be addressed reasonably promptly.
- **Low rating** represents which is in combination with other weakness and can develop into an exposure. Suggested improvements for situations not immediately/directly affecting controls.

2. ANNEXURE - 2
For Mutual Funds / Assets Management Companies (AMCs)

Table 2:

Low risk observations in current audit which were observed in previous two System audit report.

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

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

Process & Risk | Technology | Assurance | Tax | Transactions | Advisory

Gurugram

I Floor, AIHP Palms, Plot no.
242 – 243, Udyog Vihar,
Phase – IV, Gurugram,
Haryana - 122015

Mumbai

203, The Summit,
Vile Parle, Western Express
Highway, Mumbai

Hyderabad

4th Floor, Tower B, Win Win
Towers, JNTU - Hitech City Main
Road, Khanamet, Madhapur,
Hyderabad - 500 081

Pune

124, Sohrab Hall,
Sasoon Road,
Opp. Jehangir Hospital,
Pune 411001

Chandigarh

3020, Sector 46-C
Chandigarh, U. T

Amritsar

23, Anand Avenue,
Maqbool Road
Punjab

Chennai

B-403, Prince Garden,
No. 40, Thambusamy Road,
Kilpauk,
Chennai – 600 010

www.sw-india.com