CIRCULAR

SEBI/HO/MRD1/MRD1_DTCS/P/CIR/2022/58 **May 02, 2022**

To,

All Stock Exchanges,
All Clearing Corporations,
All Depositories

Dear Sir / Madam,

System and Network Audit of Market Infrastructure Institutions (MIIs)

1. Taking into account the rapid technological developments in the securities market and the entailing risks that these developments pose to the efficiency and integrity of markets, SEBI vide Circular no. SEBI/HO/MRD1/ICC1/CIR/P/2020/03 dated January 07, 2020, had mandated that stock exchanges, clearing corporations and depositories should conduct an Annual System Audit by a reputed independent auditor.

2. In order to keep pace with the technological advancements in the securities market, it is felt that there is a need to revise the aforementioned Circular. Accordingly, based on discussions with Stock Exchanges, Clearing Corporations, Depositories (hereinafter referred as 'Market Infrastructure Institutions – MIIs), and recommendations of the Technical Advisory Committee (TAC) of SEBI, the existing System Audit Framework has been reviewed.

3. MIIs are required to conduct System and Network Audit as per the framework enclosed as Annexure 1 and Terms of Reference (TOR) enclosed as Annexure 2. MIIs are also required to maintain a list of all the relevant SEBI circulars/ directions/ advices, etc. pertaining to technology and compliance

thereof, as per format enclosed as Annexure 3 and the same shall be included under the scope of System and Network Audit.

4. MIIs are also required to submit information with regard to exceptional major Non-Compliances (NCs)/ minor NCs observed in the System and Network audit as per format enclosed as Annexure 4 and are required to categorically highlight those observations/NCs/suggestions pointed out in the System and Network audit (current and previous) which remain open.

5. The Systems and Network audit Report including compliance with SEBI circulars/ guidelines and exceptional observation format along with compliance status of previous year observations shall be placed before the Governing Board of the MII and then the report along with the comments of the Management of the MII shall be communicated to SEBI within a month of completion of audit.

6. Further, along with the audit report, MIIs are required to submit a Joint declaration from the Managing Director(MD)/Chief Executive Officer(CEO) and Chief Technology Officer (CTO) certifying a) the security and integrity of their IT Systems. b) correctness and completeness of data provided to the Auditor c) entire network architecture, connectivity (including co-lo facility) and its linkage to the trading infrastructure are in conformity with SEBI's regulatory framework to provide fair equitable, transparent and non-discriminatory treatment to all the market participants d) internal review of Critical Systems as defined in SEBI circular dated March 22, 2021 was carried out during the Audit period, including the Failure Modes and Effects Analysis (FMEA).

7. This circular supersedes the abovementioned Circular no. SEBI/HO/MRD1/ICC1/CIR/P/2020/03 dated January 07, 2020. This circular is available on SEBI website at www.sebi.gov.in under the categories "Legal Framework" and "Circulars".

8. The provisions of the Circular shall come into force with immediate effect.

9. The circular is issued with the approval of the competent authority.

10. This circular is being issued in exercise of the powers conferred by Section

11(1) of Securities and Exchange Board of India Act, 1992 read with Regulation 51 of Securities Contracts (Regulation) (Stock Exchanges and Clearing Corporations) Regulations, 2018 and Section 19 of the Depositories Act, 1996 read with Regulation 97 of Securities and Exchange Board of India (Depositories and Participants) Regulations, 2018 to protect the interest of investors in securities market and to promote the development of, and to regulate the securities market.

Yours faithfully,

Ansuman Dev Pradhan
Deputy General Manager
Market Regulation Department
Email: ansumanp@sebi.gov.in

Encl.:

Annexure 1	System and Network Audit Framework
Annexure 2	Terms of Reference (TOR) for System and Network Audit Program
Annexure 3	Format for monitoring compliance with SEBI circulars/guidelines/advisories related to Technology
Annexure 4	Exception Observation Reporting Format

Annexure 1

System and Network Audit Framework

Audit Process

1. For the System and Network Audit, the following broad areas shall be considered in order to ensure that the audit is comprehensive and effective:

   a. The Audit shall be conducted according to the Norms, Terms of Reference (TOR) and Guidelines issued by SEBI.

   b. The Governing Board of the Market Infrastructure Institution (MII) shall appoint the Auditors based on the prescribed Auditor Selection Norms and TOR.

   c. An Auditor can perform a maximum of 3 successive audits. However, such auditor shall be eligible for re-appointment after a cooling-off period of two years.

   d. Further, during the cooling-off period, the incoming auditor may not include:

      (i) Any firm that has common partner(s) with the outgoing audit firm; and

      ii) Any associate / affiliate firm(s) of the outgoing audit firm which are under the same network of audit firms wherein the term "same network" includes the firms operating or functioning, hitherto or in future, under the same brand name, trade name or common control.

   e. The number of years an auditor has performed an audit prior to this circular shall also be considered in order to determine its eligibility in terms of sub-clause c above.

   f. The scope of the Audit may be broadened by the Auditor to inter-alia incorporate any new developments that may arise due to issuance of circulars/ directions/ advice by SEBI from time to time.

   g. The audit shall be conducted once in a financial year and period of audit shall be 12 months. However for the MIIs, whose systems have been identified as “protected system” by National Critical Information Infrastructure Protection Centre (NCIIPC), the audit shall be conducted on a half yearly basis and audit period shall be of 6 months. Further, the audit shall be completed within 2 months from the end of the audit period.

h. In the Audit report, the Auditor shall include its comments on whether the areas covered in the Audit are in compliance with the norms/ directions/ advices issued by SEBI, internal policy of the MII, etc. Further, the audit report shall also include specific non-compliances (NCs), observations for minor deviations and suggestions for improvement. The audit report shall take previous audit reports into consideration and cover any open items therein. The auditor should indicate if a follow-on audit is required to review the status of NCs.

i. For each of the NCs/ observations and suggestions made by the Auditor, specific corrective action as deemed fit may be taken by the MII. The management of the MII shall provide its comments on the NCs, observations and suggestions made by the Auditor, corrective actions taken or proposed to be taken along with time-line for such corrective actions.

j. The Audit report along with the comments of management shall be placed before the Governing Board of the MII. The Audit report along with comments of the Governing Board shall be submitted to SEBI, within 1 month of completion of audit.

k. The follow-on audit should be completed within one month of the corrective actions taken by the MII. After the follow-on audit, the MII shall submit a report to SEBI within 1 month from the date of completion of the follow-on audit. The report shall include updated Issue-Log to indicate the corrective actions taken and specific comments of the Auditor on the NCs and the corrective actions.

l. In cases wherein follow-on audit is not required, the MII shall submit an Action Taken Report (ATR) to the Auditor. After verification of the ATR by the Auditor, the MII shall submit a report to SEBI within 1 month from the date of completion of verification by the Auditor. The report shall include updated Issue-Log to indicate the corrective actions taken and specific comments of the auditor on the ATR.

m. The overall timeline from the last date of the audit period till completion of final compliance by MII, including follow-on audit, if any, should not exceed one year/6 months(as applicable). In exceptional cases, if MII is of the view that compliance with certain observations may extend beyond said period, then the concerned MII shall seek specific approval from the Governing Board.

Auditor Selection Norms

2. MII shall ensure compliance with the following norms while appointing Auditor:

a. The Auditor must have minimum 3 years of demonstrable experience in IT audit of securities market participants e.g. stock exchanges, clearing corporations, depositories, intermediaries, etc. and/ or financial services sector i.e. banking, insurance, Fin-tech etc.

b. The team performing system and network audit must have experience in / direct access to experienced resources in the areas covered under TOR. It is recommended that resources deployed by the Auditor for the purpose of system and network audit shall have relevant industry recognized certifications e.g. CISA (Certified Information Systems Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, GSNA (GIAC Systems and Network Auditor), CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium, commonly known as (ISC).

c. The Auditor shall have experience in working on Network audit/IT audit/governance/IT service management frameworks and processes conforming to industry leading practices like CobiT/ ISO 27001 and beyond.

d. The Auditor should have the capability to undertake forensic audit and undertake such audit as part of system and network audit, if required.

e. The Auditor must not have any conflict of interest in conducting fair, objective and independent audit of the exchange / depository/ clearing corporation. It should not have been engaged over the last three years in any consulting engagement with any departments / units of the entity being audited.

f. The Auditor should not have any cases pending against it, which point to its incompetence and/or unsuitability to perform the audit task.

g. The proposed audit agency must be empanelled with CERT-In.

h. Any criteria, in addition to the aforesaid criteria, that the MII may deem fit for the purpose of selection of Auditor.

Audit Report Guidelines

3. The Audit report should cover each of the major areas mentioned in the TOR and compliance with SEBI circulars/directions/advices, etc. related to technology. The Auditor in the Audit Report shall give its views indicating the NCs to the standards or observations or suggestions. For each section, auditors should also provide qualitative inputs/suggestions about ways to improve the processes, based upon the best industry practices.

4. The auditor shall certify that entire network architecture, connectivity (including co-lo facility) and its linkage to the trading infrastructure are in conformity with SEBI's regulatory framework to provide fair equitable, transparent and non-discriminatory treatment to all the market participants.
5. The report should also include tabulated data to show NCs / observations for each of the major areas in the TOR.
6. The audit report to include point-wise compliance of areas prescribed in Terms of Reference (TOR) and areas emanating from relevant SEBI circulars/directions/advices along with any accompanying evidence.
7. Evidences should be specified in the audit report while reporting/ closing an issue.
8. A detailed report with regard to the system and network audit shall be submitted to SEBI. The report shall include an Executive Summary as per the following format:

Issue Log Column Heading	Description	Responsibility
Major Area	Comprehensive identification of major areas in compliance with various SEBI circulars / norms and internal policies of MII	Auditor/Auditee
Point wise Compliance	Point-wise list of areas/relevant clauses in TOR against which compliance is being audited (in tabular format).	Auditor
Description of Finding/ Observation	Describe the findings in sufficient detail, referencing any accompanying evidence (e.g. procedure manual, interview notes, reports etc.)	Auditor
Reference	Reference to the section in detailed report – where full background information about the findings are available	Auditor
Process/ Unit	Process or unit where the audit is conducted and the finding pertains to	Auditor
Category of Findings	Major/Minor Non-compliance, Observation, Suggestion etc.	Auditor

Issue Log Column Heading	Description	Responsibility
Audited By	Which Auditor covered the findings	Auditor
Root Cause Analysis	A detailed analysis on the cause of the Non-compliance	Auditee
Remediation	The action (to be) taken to correct the Non-compliance	Auditee
Target Completion Date for Remedial Action	The date by which remedial action must be/will be completed	Auditor/Auditee
Status	Status of finding on reporting date (open/close)	Auditor/Auditee
Verified By	Auditing personnel (upon verification that finding can be closed)	Auditor
Closing Date	Date when finding is verified and can be closed	Auditor

Annexure 2

System and Network audit Program – Terms of Reference (TOR)

1. The scope of audit shall encompass all the IT resources including hardware, software, network, policies, procedures etc. of MIIs (Primary Data Centre (PDC), Disaster Recovery Site (DRS) and Near Site (NS))

2. **IT environment**

   2.1. Organization details

   a. Name

   b. Address

   c. IT team size (in house- employees)

   d. IT team size (vendors)

   2.2. IT and network set up and usage

   a. PDC, DRS, NS and Regional/ Branch offices (location, owned/ outsourced)

   b. Connectivity amongst PDC, NS and DRS

   c. IT infrastructure / applications pertaining to the activities done as a MII.

   d. System Architecture

   e. Network architecture

   f. Telecommunication network

3. **IT Governance**

   3.1. Whether IT Governance framework exists to include the following:

   a. IT organization structure including roles and responsibilities of key IT personnel;

   b. IT governance processes including policy making, implementation and monitoring to ensure that the governance principles are followed;

   3.2. IT policies and procedures

a. Whether the organization has a defined and documented IT policy? If yes, is it approved by the Governing Board (GB)?

b. Is the current System Architecture, including infrastructure, network and application components describing system linkages and dependencies, documented?

c. Whether defined and documented Standard Operating Procedures (SOPs) for the following processes are in place?

i. IT Assets Acquisition
ii. Access Management
iii. Change Management
iv. Backup and Recovery
v. Incident Management
vi. Problem Management
vii. Patch Management
viii. Data Centre Operations
ix. Operating Systems and Database Management
x. Network Management
xi. DRS Operations
xii. Data Retention and Disposal
xiii. Asset Inventory
xiv. IT asset refresh/replacement policy
xv. Database security
xvi. Interface Security
xvii. Application Security
xviii. Password Security
xix. Archived and backed up data security

3.3. Whether the above mentioned SOPs is reviewed at periodic intervals or upon the occurrence of any major event? In this regard, whether any organization policy has been formulated by the MII?

4. **Business Controls**

4.1. General Controls for Data Centre Facilities

a. Application Access – segregation of duties, database and application access etc. (Approved Policy clearly defining roles and responsibilities of the personnel handling business operations)

b. Maintenance Access – vendor engineers

c. Physical Access controls – permissions, logging, exception reporting & alerts

d. Environmental Controls – fire protection, AC monitoring, etc.

e. Fault Resolution Mechanism

f. Folder Sharing and Back Up Controls – safeguard of critical information on local desktops

g. Incidences of violations in the previous audit report and corrective action(s), if any, taken

h. Any other controls, as deemed fit, by the MII

4.2. Software change control

a. Whether pre-implementation review of application controls (including controls over change management) was undertaken?

b. Adherence to secure Software Development Life Cycle (SDLC) / Software Testing Life Cycle (STLC) standards/ methodologies

c. Whether post implementation review of application controls was undertaken?

d. Is the review of processes to ensure data integrity post implementation of new application or system followed by implementation team?

e. User awareness

f. Processing of new feature request

g. Fault reporting / tracking mechanism & process for resolutions

h. Testing of New releases / Bug-fixes – Testing process (automation level)

i. Version Control – History, Change Management process etc.

j. Development / Test/ Production environment – Segregation

k. New Release in Production – Promotion, Release note approvals

l. Production Issues / disruptions reported in the previous audit report, root cause analysis & corrective actions taken, if any

m. Software Development Stage

n. Software Design to ensure adequate system capacity to enable functioning in a degraded manner in the event of a crash.

o. Any other controls, as deemed fit, by the MII

4.3. Data Communication/ Network Controls

a. Network Administration – Redundancy, Monitoring, breakdown resolution etc.

b. WAN Management – Connectivity provisions for business continuity.

c. Encryption - Router based as well as during transmission

d. Connection Permissions – Restriction on need to have basis

e. Fallback Mechanism – Dial-up connections controls etc.

f. Hardware based Signing Process

g. Incidences of access violations observed in the previous report & corrective actions taken, if any

h. Any other controls, as deemed fit, by the MII

4.4. Security Controls

a. Secured e-mail with other entities such as SEBI, other partners

b. Email Archival Implementation

4.5. Access Policy and Controls

a. Defined and documented policies and procedures for managing access to applications and infrastructure –PDC, DRS, NS, branches (including network, operating systems and database) and approved by relevant authority

b. Review of access logs

c. Access rights and roles review procedures for all systems

d. Segregation of Duties (SOD) matrix describing key roles

e. Risk acceptance for violation of SOPs and alternate mechanism put in place

f. Privileged access to system and record of logs,

g. Periodic monitoring of access rights for privileged users

h. Authentication mechanisms used for access to systems including use of passwords, One Time Passwords (OTP), Single Sign on, etc.

i. Any other controls, as deemed fit, by the MII

4.6. Electronic Document Controls

4.7. General Access Controls

4.8. Performance Audit

a. Comparison of changes in transaction volumes since previous audit

b. Review of systems (hardware, software, network) performance over the period

c. Review of the current volumes against the last performance test and against the current system utilization

4.9. Business Continuity / Disaster Recovery Facilities

a. Business Continuity Planning (BCP) manual, including Business Impact Analysis (BIA), Risk Assessment and Disaster Recovery (DR) process, Roles and responsibilities of Incent Response Team (IRT) /Crisis Management Team (CMT), employees, support/outsourced staff.

b. Implementation of policies

c. Back-up procedures and recovery mechanism using back-ups.

d. Storage of Back-up (Remote site, DRS etc.)

e. Redundancy – Equipment, Network, Site etc.

f. DRS installation and Drills - Management statement on targeted resumption capability (in terms of time required & extent of loss of data)

g. Evidence of achieving the set targets during the DR drills in event of various disaster scenarios.

h. Debrief / review of any actual event when the DR/BCP was invoked during the year

i. User awareness and training

j. Is Recovery Time Objective (RTO) /Recovery Process Objective (RPO) during BIA documented?

k. Is annual review of BCP-DR or in case of major change in business/ infrastructure undertaken?

l. Is quarterly review regarding implementation of BCP policy done by Standing Committee of Technology (SCOT) of the MII?

m. Testing of BCP-DR plan through appropriate strategies including simulations, DR drills, system recovery, etc.

n. Is the recordkeeping of quarterly DR drills, live trading sessions from DRS being maintained?

o. Is BCP-DR policy document prepared and implemented in line with SEBI circular on BCP and DR of MII?

4.10. IT/Network Support & IT Asset Management

a. Utilization Monitoring – including report of prior year utilization

b. Capacity Planning – including projection of business volumes

c. Capacity and performance management process for the network/systems

d. IT (S/W, H/W & N/W) Assets, Licenses & maintenance contracts

e. Comprehensive review of Assets life cycle management (Acquisition, commissioning, deployment, monitoring, maintenance and de commissioning) and relevant records related to it.

f. Insurance

g. Disposal – Equipment, media, etc.

5. Entity Specific Software used for or in support of trading/clearing systems / peripheral systems and critical processes

6. **Human Resources Management**

6.1. Screening of Employee, Third party vendors / contractors

6.2. Onboarding

6.3. Offboarding

6.4. Consequence Management (Incident / Breach of policies)

6.5. Awareness and Trainings

6.6. Non-Disclosure Agreements (NDAs) and confidentiality agreement

7. **Network audit**

7.1 The audit shall cover entire network infrastructure which shall inter-alia includes physical verification and tracing of the connectivity paths, server configuration, physical checking wire to wire connectivity and configurations of computer networking devices etc.

7.2 The audit shall require tracing of the connectivity and network diagram based on the physical audit.

7.3 The audit shall cover the link, the path, device-level redundancy, no single-point failures, high availability, and fault tolerance aspects in the network.

7.4 The audit shall cover entire network that is used to connect members to the MIIs (POP, MPLS, VSAT, COLO, etc.)

7.5 The audit shall cover applications, internal networks, servers, etc. of the MIIs/offered by the MIIs to its members that are used for trading, risk management, clearing and settlement etc.

7.6 Network performance and design

7.7 Network Security implementation

7.8 Network health monitoring and alert system

7.9 Log management process

7.10 Service level definition for vendors/Service level management

7.11 Governance process for network service delivery by vendors

8. The results of all testing that was conducted before deployment of any IT system/application in production environment, shall be checked by auditor during system audit. .

9. **IT Vendor Selection and Management**
   - 9.1. Identification of eligible vendors
   - 9.2. Dissemination process of Request for Proposal (RFP)
   - 9.3. Definition of criteria of evaluation
   - 9.4. Process of competitive analysis
   - 9.5. Approach for selection
   - 9.6. Escrow arrangement for keeping source code

10. **E-Mail system**
    - 10.1. Existence of policy for the acceptable use of electronic mail
    - 10.2. Regulations governing file transfer and exchange of messages with external parties
    - 10.3. Rules based on which e-mail addresses are assigned
    - 10.4. Storage, backup and retrieval

11. **Redressal of Technological Complaints**
    - 11.1. Ageing analysis of technology complaints
    - 11.2. Whether all complaints received are brought to their logical conclusion?

12. **Any other Item(s)**
    - 12.1. Electronic Waste Disposal
    - 12.2. Observation(s) based on previous Audit Report (s)
    - 12.3. Any other specific area(s) that may be informed by SEBI.

Annexure 3

Format for monitoring compliance with requirements emanating from SEBI circulars/guidelines/advisories related to technology

Sl. No.	Date of SEBI circular/ directions/ advice, etc.	Subject	Technological requirements specified by SEBI in brief	Mechanism put in place by the MIIs	Non compliances with SEBI circulars/ directions, etc.	Compliance status (Open/ closed)	Comments of the Management	Time-line for taking corrective action in case of open observations

Annexure 4

Exception Observation Reporting Format

Note: MIIs are expected to submit following information with regard to exceptional major non-compliances (NCs) / minor NCs observed in the System and Network Audit. MIIs should also categorically highlight those observations/NCs/suggestions pointed out in the System and Network Audit (current and previous) which are not yet complied with.

Name of the MII: ____________________

Name of the Auditor: ____________________

Systems and Network Audit Report Date: ____________________

Table 1: For preliminary audit

Audit period	Observation No.	Description of finding	Department of MII	Status/ Nature of finding	Risk Rating of finding as per Auditor	Audit TOR clause	Root Cause Analysis	Impact Analysis	Corrective Actions proposed by auditor	Deadline for the corrective action	Management response in case of acceptance of associated risks	Whether similar issue was observed in any of the previous 3 Audits

Description of relevant Table heads

1. **Audit Period** – This indicates the period of audit

2. **Description of findings/observations** – Description of the findings in sufficient details, referencing any accompanying evidence

3. **Status/ Nature of Findings** – The category can be specified, for example:

    a. Non-compliant (Major/Minor)

    b. Work in progress

    c. Observation

    d. Suggestion

4. **Risk Rating of finding** - A rating has to be given for each of the observations based on its impact and severity to reflect the risk exposure as well as the suggested priority for action

Rating	Description
HIGH	Represents weakness in control with respect to threat(s) that is /are sufficiently capable and impacts asset (s) leading to regulatory non-compliance, significant financial, operational and reputational loss. These observations need to be addressed with utmost priority.
MEDIUM	Represents weakness in control with respect to threat(s) that is /are sufficiently capable and impacts asset (s) leading to exposure in terms of financial, operational and reputational loss. These observations need to be addressed reasonable timeframe.
LOW	Represents weaknesses in control, which in combination with other weakness can develop into an exposure. Suggested improvements for situations not immediately/directly affecting controls. .

5. **Audit TOR clause –** The TOR clause corresponding to this observation

6. **Root Cause analysis** – A detailed analysis on the cause of the non-conformity.

7. **Impact Analysis** – An analysis of the likely impact on the operations/ activity of the organization

8. **Corrective Action** – The action taken to correct the non-conformity

Table 2: For follow on/ follow up system and Network audit

Preliminary Audit Date	Preliminary Audit Period	Preliminary Observation Number	Preliminary Status	Preliminary Corrective Action as proposed by Auditor	Current Finding	Current Status	Revised Corrective Action, if any	Deadline for the Revised Corrective Action	Reason for delay in implementation/ compliance

Description of relevant Table heads

1. **Preliminary Status** – The original finding as per the preliminary System and Network Audit Report

2. **Preliminary Corrective Action** – The original corrective action as prescribed in the preliminary System and Network audit report

3. **Current Finding** – The current finding w.r.t. the issue

4. **Current Status** – Current Status of the issue viz. compliant, non-compliant, work in progress (WIP)

5. **Revised Corrective Action** – The revised corrective action prescribed w.r.t. the Non-compliant/ WIP issues