Annexure 1

System Audit Framework

Audit Process

1. For the System 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/Clearing Corporations(CCs). Professional Clearing Members(PCMs) shall select the Auditors based on the prescribed Auditor Selection Norms and TOR. The Governing Board of the PCMs shall approve the appointment of the Auditors.

   b. 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.

   c. 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.

   d. 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-clauses b and c above.

   e. 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/Clearing Corporation from time to time.

   f. The audit shall be conducted for each financial year. Further, the audit shall be completed within 2 months from the end of the audit period. The Audit report shall be submitted to CCs within one month of completion of the Audit, after approval of the Governing Board (or equivalent governance structure as applicable to the entity). PCMs, who have conducted clearing activities during the audit period are liable for submission of the System Audit report.

g. 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, Clearing Corporation, internal policy of the PCM, 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.

h. For each of the NCs/ observations and suggestions made by the Auditor, specific corrective action as deemed fit may be taken by the PCM. The management of the PCM 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.

i. The Audit report along with the comments of management shall be placed before the Governing Board (or equivalent governance structure as applicable to the entity) of the PCM. The Audit report along with comments of the Governing Board shall be submitted to Clearing Corporation, within one month of completion of audit.

j. The follow-on audit should be completed within one month of the corrective actions taken by the PCM. After the follow-on audit, the PCM shall submit a report to CC within one 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.

k. In cases wherein follow-on audit is not required, the PCM shall submit an Action Taken Report (ATR) to the Auditor. After verification of the ATR by the Auditor, the PCM shall submit a report to Clearing Corporation within one 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.

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

m. The auditee team, who is responsible for direct liaison with the system auditor, at least one of the members must have thorough knowledge and experience in handling system audit.

Auditor Selection Norms

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

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

   b. The team performing system 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 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 audit, if required.

   e. The Auditor must not have any conflict of interest in conducting fair, objective and independent audit of the PCM. 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 on the date of appointment as auditor and date of submission of audit report.

   h. Any criteria, in addition to the aforesaid criteria, that the PCM 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 and CC 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 report should also include tabulated data to show NCs / observations for each of the major areas in the TOR.
5. The audit report to include point-wise compliance of areas prescribed in TOR and areas emanating from relevant SEBI and CC circulars/directions/advices along with any accompanying evidence.
6. Evidences should be specified in the audit report while reporting/ closing an issue.
7. A detailed report with regard to the system audit shall be submitted to CC. The report shall include an Executive Summary as per the following format:

Issue	Description	Responsibility
Major Area	Comprehensive identification of major areas in compliance with various SEBI & Clearing Corporation circulars / norms and internal policies of PCM	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

****

Annexure 2

System 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 PCMs (Primary Data Centre (PDC), Disaster Recovery Site (DRS) and Near Site (NS), if applicable).
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), if applicable

b. Connectivity amongst PDC, NS and DRS, if applicable

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

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)/Policy 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. Database security
xv. Password Security
xvi. Archived and backed up data security

3.3. Whether the above mentioned SOPs/Policies are reviewed at periodic intervals or upon the occurrence of any major event.

3.4. In this regard, whether any organization policy has been formulated by the PCM.

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 PCM

4.2. Risk Management System (RMS)

a. Risk management capability – The system auditor should check whether system of risk management including upfront real-time risk management if applicable is in place.

b. Back testing for effectiveness of RMS – Whether system has capability to identify trades which have exceeded the pre-defined limits (Order Quantity and Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order Limit, Order Price limit) and also exceeded corresponding margin availability of clients. Whether deviations from such pre-defined limits are captured by the system, documented and corrective steps taken.

c. Log Management – Whether the system maintains logs of alerts / changes / deletion / activation / deactivation of client codes and logs of changes to the risk management parameters mentioned above. Whether the system allows only authorized users to set the risk parameter in the RMS.

4.3. 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. Software Testing framework, methodology and process guideline

p. Any other controls, as deemed fit, by the PCM

4.4. Data Communication/ Network Controls

a. Network Administration – Link, Path, Redundancy, No single point of failure, high availability, fault tolerance, Monitoring, breakdown resolution etc.

b. WAN Management – Connectivity provisions for business continuity.

c. Connection Permissions – Restriction on need to have basis

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

e. Any other controls, as deemed fit, by the PCM

4.5. Security Controls

a. Email Archival Implementation

b. Anti-virus and malware controls

4.6. Access Policy and Controls

a. Defined and documented policies and procedures for managing access to applications and infrastructure –PDC, DRS, NS (if applicable) , 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. BYOD (bring your own device) policies

j. Any other controls, as deemed fit, by the PCM

4.7. Performance Audit

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

b. Current system utilization

4.8. 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 Incident Response Team (IRT) /Crisis Management Team (CMT), if applicable, 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., if applicable

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

i. User awareness and training

j. Is Recovery Time Objective (RTO) /Recovery Process Objective (RPO) during Business Impact Assessment (BIA) documented, if applicable?

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

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

4.9. 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 of Equipment, media, and other electronic waste as per applicable waste disposal guidelines etc.

4.10. Segregation of Data and Processing facilities – The system auditor should check and comment on the segregation of data and processing facilities in case the member is also running other business.

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. 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.

8. **IT Vendor Selection and Management**

8.1. Identification of eligible vendors

8.2. Dissemination process of Request for Proposal (RFP)

8.3. Definition of criteria of evaluation

8.4. Process of competitive analysis

8.5. Approach for selection

8.6. Escrow arrangement for keeping source code

9. **E-Mail system**

9.1 Existence of policy for the acceptable use of electronic mail

9.2 Regulations governing file transfer and exchange of messages with external parties

9.3 Rules based on which e-mail addresses are assigned

9.4 Storage, backup and retrieval

10. **Redressal of Technological Complaints**

10.1 Ageing analysis of technology complaints

10.2 Whether all complaints received are brought to their logical conclusion?

11. **Any other Item(s)**

11.1 Observation(s) based on previous Audit Report (s)

11.2 Any new direction/instruction that may be informed by Clearing Corporation and/or SEBI.

****

Annexure 3

Format for monitoring compliance with requirements emanating from SEBI and Clearing Corporation (CC) circulars/guidelines/advisories related to technology

Sl. No.	Date of SEBI/CC circular/ directions/ advice, etc.	Subject	Technological requirements specified by SEBI/CC in brief	Mechanism put in place by the PCMs	Non compliances with SEBI/CC 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: PCMs are expected to submit following information with regard to exceptional major non-compliances (NCs) / minor NCs observed in the System Audit. PCMs should also categorically highlight those observations/NCs/suggestions pointed out in the System Audit (current and previous) which are not yet complied with.

Name of the PCM: ___________________

Name of the Auditor: _________________

Systems Audit Report Date: _________________

Table 1: For preliminary audit

Audit period	Observation No.	Description of finding	Department of PCM	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 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 Audit Report

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

****