NSDL
Technology, Trust & Reach

**Participant Services Circular**

Circular No.: NSDL/POLICY/2026/0087 June 04, 2026

**Subject: Implementation of SEBI CSCRF Circular for submission of the Annual System Audit Report.**

Attention of Participants is invited to SEBI Circular No. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 regarding "Cyber Security & Cyber Resilience Framework for Stockbrokers / Depository Participants" (ref: NSDL Circular No. NSDL/POLICY/2018/0069 dated December 6, 2018) and NSDL Circular No. NSDL/POLICY/2024/0132 dated September 18, 2024 regarding submission of the annual system audit report.

In this regard, Participants are hereby informed that, the 'qualifications and criteria for selection and appointment of auditors for conducting system audit' and 'Terms of Reference (TOR) for the system audit report' as provided in NSDL Circular No. NSDL/POLICY/2024/0132 dated September 18, 2024 has been revised and are provided as **Annexure A** and **Annexure B** to this Circular.

Participants are requested to take note of the periodicity and due date of submission of the annual system audit report as mentioned in the table given below. Moreover, for each non-compliance reported by the auditor, Participants are required to submit corrective Action Taken Report (ATR) as per below mentioned timelines:

| Report | Periodicity/ Frequency | Due date of submission initial report | Action Taken Report (ATR) submission (if applicable) |
|---|---|---|---|
| Annual System Audit Report | Annually | Within three months from the end of the financial year i.e. by 30th June. | Within three months from the due date of submission i.e. by 30th September. |

Further, the auditor shall provide compliance status for each TOR item as Compliant/Non-Compliant/Not Applicable and in case of any TOR item which is not applicable, auditor is required to provide justification for the non-applicability of said TOR.

Participants are requested to take note that, for each non-compliance reported by the auditor is required to submit corrective action taken report and same shall be validated by the same auditor who conducted

the system audit as per the above-mentioned timelines. On review of details of corrective action submitted by Depository Participant members, the auditor shall submit the status of compliance as Compliant or Non-Compliant on web portal.

Further, guidelines for submission of reports on online portal details shall be communicated through a separate circular.

Participants are advised to take note of the above to bring the provisions of this circular to the notice of the auditors and put in place adequate systems and procedures to ensure strict adherence to the compliance requirements.

Participants are further advised to note that non-submission of Annual System Audit Report within the specified timelines shall be treated as regulatory non-compliance and may attract penalty and/or further action, as per the NSDL Business Rules, as amended from time to time.

For any clarifications in this regard, Participants may write to **dpaudit@nsdl.com** or contact us at (022-42165062) (022-42165038). Participants are requested to take note of above circular and ensure compliance.

**For and on behalf of**
**National Securities Depository Limited**

Rakesh Mehta Digitally signed by Rakesh Mehta
Date: 2026.06.04 18:43:28 +05'30'

**Rakesh Mehta**
**Vice President**

Enclosures: Two

| FORTHCOMING COMPLIANCE | | | |
|---|---|---|---|
| **Particulars** | **Deadline** | **Manner of sending** | **Reference** |
| Investor Grievance Report (Monthly) | By 10th of the following month | Through e-PASS | Para 22 of 'Grievance Redressal' chapter and Para 27 of 'Internal Controls/Reporting to NSDL/SEBI' chapter of NSDL Master Circular for Participants |
| Compliance report w.r.t Same Mobile number and/ or email address captured for multiple accounts. (Monthly) | Before 27th of following month | Through Email. | Para 26 of 'Miscellaneous' chapter of NSDL Master Circular for Participants. |
| Artificial Intelligence /Machine Learning Reporting Form (Annually) | Within three months of the end of the financial year | Through e-PASS | Para 10 of 'Internal Controls/Reporting to NSDL/SEBI' chapter of NSDL Master Circular for Participants |
| Annual System Audit Report (yearly) | June 30th | Through e-PASS | Para 20.5 of 'Internal Controls/Reporting to NSDL/SEBI' chapter of NSDL Master Circular for Participants |
| Annual Cyber Audit Report (yearly) | June 30th | Through e-Pass | Para 2.76 of 'Internal Controls/Reporting to NSDL/SEBI' chapter of NSDL Master Circular for Participants and Circular No.: NSDL/POLICY/2026/0074 dated May 12, 2026 |

NSDL
Technology, Trust & Reach

**Participant Services Circular**

## Annexure A

## Auditor Selection Norms

1. The Auditor should have experience of IT audit/governance frameworks and processes conforming to industry leading practices like COBIT 5/ISO 27001.
2. An Auditor/Audit firm/LLP/Company having 3 years or more experience, can take assignment of conducting system audit of securities market participants. The audit experience should cover all the major areas mentioned under Terms of Reference (ToR) of the system audit specified by SEBI / depositories.
3. The Auditor/Audit firm can perform a maximum of 3 successive audits of the DP.
However, such an auditor shall be eligible for re-appointment after a cooling-off period of two years.
4. The appointed Auditor and Audit Firm/LLP/Company's resources should possess at least one of the following certifications:
• CISA (Certified Information System Auditors) from ISACA
• DISA (Post Qualification Certification in Information Systems Audit) from
Institute of Chartered Accountants of India (ICAI)
• CISM (Certified Information Security Manager) from ISACA
• CISSP (Certified Information Systems Security Professional) from International
Information Systems Security Certification Consortium, commonly known as (ISC2).
5. The Auditor/Audit Firm/LLP/Company, as being appointed by the DP must not have any conflict of interest in conducting fair, objective, and independent audit. Further, the Directors/Partners/Proprietor of Audit firm shall not be related to any Directors/Promoters/Proprietor of the said DPs either directly or indirectly.
6. Auditor/Audit Firm/LLP/Company shall not have any cases pending against its previous system audit assignments of DPs, which point to its incompetence and/or unsuitability to perform the audit task.
7. The DP and Auditor/Audit Firm/LLP/Company are required to retain records of physical visits conducted during audits like name, qualification & date of visit/s of auditor, along with audit artifacts, proofs of concept (POCs), and evidence related to Terms of Reference (TOR) points for a minimum duration of three years.
8. The Auditor/Audit Firm/LLP/Company is not debarred or restrained from issuing any certificate by ICAI, ISACA, ISC2, RBI, SEBI, Cert-In or by other regulator/law enforcement agency.

**Annexure B**

**Terms of Reference (TOR) for System Audit**

| Audit TOR Clause | TOR Status |
|---|---|
| **1** | **Software Change Management - The system auditor should check whether proper procedures have been followed, and proper documentation has been maintained for the following:** |
| 1(a) | Processing / approval methodology of new feature request, change or patches |
| 1(b) | Change Management Process, related approvals, Version Control- History, etc.<br>For change requests, whether the changes are tested before being approved for deployment into production.<br>Whether the categorization of the change is done properly? |
| 1(c) | Testing of new releases / patches / modified software / bug fixes (Automation Level) |
| 1(d) | Testing of new releases / patches / modified software / bug fixes<br>Does demonstratable segregation exists between Development / Test / Production environment |
| 1(e) | The System Auditor to check whether adequate mechanism to restore their application systems to 'production state' at the end of testing session so as to ensure integrity of application system. |
| 1(f) | New release in production – promotion, release note approvals |
| 1(g) | Production issues / disruptions reported during last year, reasons for such disruptions and corrective actions taken. |
| 1(h) | User Awareness |
| 1(i) | Change Management - To ensure system integrity and stability all changes to the installed system are planned, evaluated for risk, tested, approved and documented. Has the organisation implemented a change management process to avoid risk due to unplanned and unauthorised changes for all the information security assets (Hardware, software, network, application)? Does the process at the minimum include the following? Planned Changes Are changes to the installed system made in a planned manner? a) Are they made by duly authorized personnel? b) Risk Evaluation Process c) Is the risk involved in the implementation of the changes duly factored in? Change |

| Audit TOR Clause | TOR Status |
|---|---|
| | Approval Is the implemented change duly approved, and process documented? Pre-implementation process Is the change request process documented? Change implementation process Is the change implementation process supervised to ensure system integrity and continuity. Post-implementation process Is user acceptance of the change documented? Emergency Changes In case of emergency changes, are the same duly authorized and the manner of change documented later? Are Records of all change requests maintained? Are periodic reviews conducted for all the changes which were implemented? |
| 1(j) | Patch Management - Does the organization have a documented process/procedure for timely deployment of patches for mitigating identified vulnerabilities? Does the organisation maintain a tracker for the deployed, failed or missing patches along with the dates of the patch being applied? Whether version and patch management controls are in place? Does the organization periodically update all assets including Servers, OS, Database, Middleware, Network Devices, Firewalls, IDS /IPS Desktops etc. with latest applicable versions and patches? Ensure that the critical system (servers, network devices, Endpoints) are replaced before they reach End-of-Life or End-of-support and no EOL/EOS systems are present in the Member's environment. |
| 1(k) | SDLC - Application Development & Maintenance In case of members self-developed system SDLC documentation and procedures if the installed system is developed in-house. |
| 1(l) | SDLC - Application Development & Maintenance<br>Does the organization has any in house developed applications?<br>If Yes , then Does the organization have a documented process/framework to include processes for incorporating, testing and providing sign-off for information risk requirements at various stages of Software Development Life Cycle (SDLC)?<br>Does the SDLC framework incorporate standards, guidelines and procedures for secure coding?<br>Are roles and responsibilities clearly defined for various stakeholders in the SDLC framework?<br>Are Application development, Testing (QA and UAT) and Production environments segregated? |
| 1(m) | Changes undertaken pursuant to a change to the depository applications. |

| Audit TOR Clause | TOR Status |
|---|---|
| **2** | **Password Security** |
| 2(a) | Organization Access Policy<br>Whether the organization has a well-documented policy that provides for a password policy as well as access control policy for the depository applications / Depository Participant's systems |
| 2(b) | Authentication Capability – Whether the system authenticates user credentials by means of a password before allowing the user to login, and whether there is a system for authentication of orders originating from Internet Protocol by means of two-factor authentication, including Public Key Infrastructure (PKI) based implementation of digital signatures. |
| 2(c) | Password Best Practices – Whether there is a system provision for masking of password, system prompt to change default password on first login, disablement of user id on entering multiple wrong passwords (as defined in the password policy document), periodic password change mandate and appropriate prompt to user, strong parameters for password, deactivation of dormant user id, etc. |
| 2(d) | The installed depository applications is as per the guidelines as per the depository. The installed applications use password for authentication. The password policy/standard is documented. The installed systems password features includes: a) The installed system uses passwords for authentication. b) The system requests for identification and new password before login into the system. c) The Password is masked at the time of entry. System authenticates user with a User Name and password as first level of security. System mandates changing of password when the user logs in for the first time? Automatic disablement of the user on entering erroneous password on five consecutive occasions. The system provides for automatic expiry of passwords at the end of a reasonable duration (maximum 90 Days) and re-initialisation of access on entering fresh passwords. Prior intimation is given to the user before such expiry? System controls to ensure that the password is alphanumeric (preferably with one special character), instead of just being alphabets or just numerical. System controls to ensure that the changed password cannot be the same as of the last 6 passwords. System controls to ensure that the Login id of the user and password should not be the same. System controls to ensure that the password should be of minimum six characters. User/Client is deactivated if the same is not used for a continuous period |

| Audit TOR Clause | TOR Status |
|---|---|
| | of 24 (Twenty four) months from date of last use of the account. System allows user to change their passwords at their discretion and frequency. System controls to ensure that the password is encrypted at member's end so that employees of the member cannot view the same at any point of time. |
| **3** | **Session Management (Mobile Application / Applicability Client Server Application / Web Application)** |
| 3(a) | Session Authentication – Whether the system has provision for Confidentiality, Integrity and Availability (CIA) of the session and the data transmitted during the session by means of appropriate user and session authentication mechanisms like SSL etc. |
| 3(b) | Session Security - Whether there is availability of an end-to-end encryption for all data exchanged between client and Depository Participant's systems or any other means of ensuring session security? Whether session login details are stored securely? |
| 3(c) | Inactive Session - Whether the system allows for automatic session logout after a system defined period of inactivity? |
| 3(d) | Log Management – Whether the system generates and maintain logs of Number of users, activity logs, system logs, Number of active clients. |
| 3(e) | Whether the installed system has provision for security, reliability and confidentiality of data through use of encryption technology, SSL or similar session confidentiality protection mechanisms:<br>a) The system uses SSL/TLS or similar session confidentiality protection mechanisms<br>b) The system uses a secure storage mechanism for storing of usernames and passwords<br>c) The system adequately protects the confidentiality of the user's data |
| 3(f) | Cryptographic Controls - Does the organization have a documented process/framework for implementing cryptographic controls in order to protect confidentiality and integrity of sensitive information during transmission and while at rest, using suitable encryption technology? Is the encryption methodology of information involved in business transactions based on Regulation/Law/Standards compliance requirements? Does the organization ensure Session Encryption for internet based applications including the following? Does the organization ensure that |

| Audit TOR Clause | TOR Status |
|---|---|
| | the data transferred through internet is protected with suitable encryption technologies? Are transactions on the website suitably encrypted? |
| 3(g) | Cryptographic Controls - Is secret and confidential information sent through e-mails encrypted before sending? Is secret and confidential data in an encrypted format? |
| 3(h) | Does the organization have deployed data loss prevention (DLP)solutions / processes? Is the DLP configured/ deployed across all the endpoints (end users), email and network? Are relevant policies/ rules configured on the DLP to prevent exfiltration of PII data, sensitive and confidential data from within the organisation and organisational assets? Does the DLP solution / process support alerting / blocking of movement of data from within the organisation to an unauthorised external domain? |
| **4** | **Database Security** |
| 4(a) | Access - Whether the system allows database access only to authorized users / applications. |
| 4(b) | Controls - Whether the database server is hosted on a secure platform, with username and password stored in an encrypted form using strong encryption algorithms. |
| 4(c) | Data at rest is encrypted |
| **5** | **Network Integrity** |
| 5(a) | Seamless connectivity – Whether Depository Participant has ensured that a backup network link is available in case of primary link failure with the exchange. |
| 5(b) | Network Architecture – The member should have detailed network architecture diagram delineating depository connectivity along with the backup links to showcase failover, clear portrayal of internet service providers, segregation of different zones (Production, UAT, DMZ, etc.). The network diagram should also depict the internal and external flow of network traffic. The version control should be maintained for the Network Diagram. The Network Architecture diagram should be periodically reviewed or in case of any changes to the infrastructure. The Network Architecture diagram should also be approved by the Technology Committee. |
| 5(c) | Firewall Configuration – Whether appropriate firewall is present between Depository Participant trading setup and various communication links to the exchange. Whether the firewall default configuration settings are changed and is appropriately configured to ensure maximum security. |

| Audit TOR Clause | TOR Status |
|---|---|
| 5(d) | Network Security - Are networks segmented into different zones as per security requirements? Whether the organization has installed network security devices, such as WAF (web application firewall), proxy servers, IPS, etc. to protect their IT infrastructure which is exposed to the internet, from security exposures originating from internal and external sources. Has the organization implemented suitable monitoring tools to monitor the traffic within the organization's network and to and from the organizations network? Does the organization periodically conduct Network Architecture Security assessments in order to identify threats and vulnerabilities? Are the findings of such assessments tracked and closed? Are Internet facing servers placed in a DMZ and segregated from other zones by using a firewall? Is there segregation between application and database servers? Are specific port/service accesses granted on firewall by following a proper approval process? Are user and server zones segregated? Are the rules defined in the firewall adequate to prevent unauthorized access to depository applications and back office systems? |
| **6** | **Access Controls** |
| 6(a) | Access to server rooms – Whether adequate controls are in place for access to server rooms and proper audit trails are maintained for the same. |
| 6(b) | Additional Access controls – Whether the system provides for any authentication/two factor authentication mechanism to access to various components of the depository applications and back office systems. Whether additional password requirements are set for critical features of the system. Whether the access control is adequate. |
| 6(c) | Access Control - Does the organization's documented policy and procedure include the access control policy? Is access to the information assets based on the user's roles and responsibilities? Does the system have a password mechanism which restricts access to authenticated users? Does the system request for identification and new password before login into the system? Does the system have appropriate authority levels to ensure that the limits can be setup only by persons authorized by the risk / compliance manager? Does the organization ensure that access control between website hosting servers and internal networks is maintained? Are records of all accesses requested, approved, granted, terminated and changed maintained? Are all accesses granted reviewed periodically? Does the organization ensure that default system credentials are disabled/locked? Are Application development, Testing (QA |

| Audit TOR Clause | TOR Status |
|---|---|
| | and UAT) and Production environments segregated? Whether adequate controls have been implemented for admission of personnel into the server rooms / place where servers / hardware / systems are located and whether audit trails of all the entries/exits at the server room / location are maintained? Is access to the information assets based on the user's roles and responsibilities? Does the system have a password mechanism which restricts access to authenticated users? |
| 6(d) | Extra Authentication Security - If the systems uses additional authentication measures like smart cards, biometric authentication or tokens etc. |
| 6(e) | Physical & Environmental Security - Does the organization have a documented process/framework for Physical & Environmental Security? Are adequate provisions in respect of physical security of the hardware / systems at the hosting location and controls on admission of personnel into the location (audit trail of all entries-exits at location etc.)? Are security perimeters defined based on the criticality of assets and operations? Are periodic reviews conducted for the accesses granted to defined perimeters? Are CCTV cameras deployed for monitoring activities in critical areas? Is the CCTV footage backed up, and can it be made available in case the need arises? Are suitable controls deployed for combating fire in Data Center? Does the organization maintain physical access controls for Server Room/Network Room security (environmental controls) Server Room, Network Room Security (UPS), Server room, network room security (HVAC). Are records maintained for the access granted to defined perimeters? Are suitable controls deployed for combating fire in the data center? |
| 6(f) | Privileged Identity Management - Does the organization have a documented process/procedure for defining reviewing and assigning the administrative roles and privileges? Has the organization implemented controls/tools for Privilege Identity Management including at a minimum provisioning, maintenance, monitoring, auditing and reporting all the activities performed by privileged users (Sys Admin, DBA etc.) accessing organization's IT systems? Are Privileges granted to users based on appropriate approvals and in accordance with the user's role and responsibilities? Are all the activities of the privileged users logged? Are log reviews of privileged user logs of admin activity conducted periodically? Is Maker- Checker functionality implemented |

| Audit TOR Clause | TOR Status |
|---|---|
| | for all changes by admin? Are records of privileged user provisioning/deprovisioning reviewed? |
| 6(g) | Closed User Group Endpoint Security 1- Does the member have policies and procedures having coverage related to People, Processes and Technology? 2- Does the member have architecture that supports segregation such as Business - stock broking & Other business of stockbroker Data and Processing facilities, Development / Test / Production environment, Corporate user and Production / server zones, Application and Database servers, Internet facing servers placed in a DMZ and segregated from other zones Ensure appropriately configured firewalls are used to ensure segregation wherever needed. 3- Are technology related Baseline Controls established, exercised, and reviewed periodically 4- are following systems and processes existing and exercised for Vulnerability Assessment and Penetration Testing, Configuration of Technologies prior to go live, Monitoring of perimeter / network security, infrastructure and applications for anomalies alerts incidents and breaches, Reporting of cyber-attacks, threats, cyber-incidents and breaches experienced and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities, threats to be submitted to Depository and other regulatory agencies based on applicability. |
| **7** | **Backup and Recovery** |
| 7(a) | Backup and Recovery Policy – Whether the organization has a well documented policy on periodic backup of data generated from the broking operations. |
| 7(b) | Log generation and data consistency - Whether backup logs are maintained and backup data is tested for consistency. |
| 7(c) | System Redundancy – Whether there are appropriate backups in case of failures of any critical system components. |
| 7(d) | Backup & Restoration - The Installed systems backup capability is adequate as per the requirements of the Exchange for overcoming loss of product integrity. Are backups of the following system generated files maintained as per the Exchange guidelines? At the server/gateway level a) Database b) Audit Trails Reports At the user level a) Market Watch b) Logs c) History d) Reports e) Audit Trails f)Alert logs Does the audit trail capture the record of control parameters, orders, trades and data points emanating from trades executed through algorithm trading? Does the organization ensure that the |

| Audit TOR Clause | TOR Status |
|---|---|
| | audit trail data maintained is available for a minimum period of 5 years? Does the organization ensure that the user details including username, unique identification of user, authorization levels for the users activated for algorithm facilities maintained and is available for a minimum period of 5 years? Does the audit trail for SOR capture the record of orders, trades and data points for the basis of routing decision? Are backup procedures documented, and backup logs maintained? Are the backup logs maintained and are the backups been verified and tested? Are the backup media stored safely in line with the risk involved? Are there any recovery procedures and have the same been tested? Are the backups restored and tested periodically to ensure adequacy of backup process and successful restoration? |
| 7(e) | Audit trail, Event logging and monitoring<br>o Member should maintain logs of all trading activity to facilitate audit trail.<br>o Whether system generates, captures and maintains audit trail of all transactions for at least 3 years?<br>o Audit trail should capture record of control parameters, orders, trades and data points emanating from trades executed through algorithmic trading?<br>o All events, changes in master, strategy parameters shall be logged and maintained for at least 3 years.<br>o Whether all logs generated are secured from unauthorized modifications? |
| 7(f) | How will the organization assure customers prompt access to their securities in the event the organization determines it is unable to continue its business in the primary location - Network / Communication Link Backup. Is the backup network link adequate in case of failure of the primary link to the Depository. Is the backup network link adequate in case of failure of the primary link connecting the users. Is there an alternate communications path between customers and the firm. Is there an alternate communications path between the firm and its employees. Is there an alternate communications path with critical business constituents, banks, and regulators. Whether detailed network diagram is prepared and available for verification. Is network and network diagram in line with each other. Does the organization have alternate means of communication including channel for communication for communicating with the clients in case of any disruption. Such communication should be completed within 30 minutes from the time of disruption. |

| Audit TOR Clause | TOR Status |
|---|---|
| 7(g) | How will the organization assure customers prompt access to their securities in the event the organization determines it is unable to continue its business in the primary location - System Failure Backup Are there suitable backups for failure of any of the critical system components like a) Gateway / Database Server b) Router c) Network Switch Infrastructure breakdown backup Are there suitable arrangements made for the breakdown in any infrastructure components like d) Power Supply e) Water f) Air Conditioning Primary Site Unavailability Have any provision for alternate physical location of employees been made in case of non-availability of the primary site Disaster Recovery Are there suitable provisions for Books and records backup and recovery (hard copy and electronic). Have all mission-critical systems been identified and provision for backup for such systems been made? |
| **8** | **BCP/DR (Only applicable for Depository Participants having BCP / DR site)** |
| 8(a) | BCP / DR Policy - Whether the Depository Participant has a well-documented BCP/ DR policy and plan. The system auditor should comment on the documented incident response procedures and observation on the DR drills conducted by the Depository Participant. |
| 8(b) | Alternate channel of communication – Whether the Depository Participant has provided its clients with alternate means of communication including channel for communication in case of a disaster. Whether the alternate channel is capable of authenticating the user after asking for additional details or OTP (One-Time-Password). |
| 8(c) | High Availability – Whether BCP / DR systems and network connectivity provide high availability and have no single point of failure for any critical operations as identified by the BCP/DR policy. |
| 8(d) | Connectivity with other FMIs – The system auditor should check whether there is an alternative medium to communicate with Depositories and other FMIs. |
| 8(e) | Business Continuity - Does the Organisation have a suitable documented Business Continuity or Disaster Recovery or Incident Response process commensurate with the organization size and risk profile to ensure a high degree of availability of the installed system Is there any documentation on Business Continuity / Disaster Recovery / Incident Response? If a BCP/DRP plan exists, has it been tested on regular basis? Are there any documented risk assessments? Does the installation have a Call List for |

| Audit TOR Clause | TOR Status |
|---|---|
| | emergencies maintained? Whether redundancy is built at all levels of infrastructure? Whether all critical systems / infrastructure are in HA mode? |
| 8(f) | Security Incident & Event Management - Does the organization have a documented process/policy for Security Incident & Event Management? Does the organization has a documented process/procedure for identifying Security related incidents by monitoring logs generated by various IT assets such as Operating Systems, Databases, Network Devices, etc.? Are all events/incidents detected, classified, investigated and resolved? Are periodic reports published for various identified Security incidents? Does the organization ensure that the logging facilities and the log information Are protected from tampering and unauthorized access? |
| 8(g) | Security Incident & Event Management - Is there a dedicated Incident Response Team for managing risk and compliance activities? |
| 8(h) | Business Continuity - Does the organization have a Disaster Recovery Site? Are there any documented risk assessments? Does the installation have a Call List for emergencies maintained? Does the organization have robust systems and technical infrastructure in place in order to provide essential facilities, perform systemically critical functions relating to securities market and provide seamless service to their clients? |
| 8(i) | The system auditor should comment on the documented incident response procedures which will cover the following:<br>Identification of all critical operations of the Member including the process of informing clients in case of any disruptions.<br>While putting in place the BCP/DRP, Members are advised to sufficiently review all potential risks along with its impact on the business.<br>Declaration of incident as a “Disaster” viz. timelines etc. and restoration of operations from DR Site upon declaration of ‘Disaster’ Adequate resources (with appropriate training and experience) should be available at the DR Site to handle all operations during disasters.<br>The declaration of disaster shall be reported in the preliminary report submitted to the Depository. |
| 8(j) | 1. Does the organisation have distinct primary and disaster recovery sites (DRS) for technology infrastructure, workspace for people and operational processes? |

| Audit TOR Clause | TOR Status |
|---|---|
| | Does the organisation have DRS set up sufficiently away (not less than 250 km), from Primary Data Centre (PDC) to ensure that both DRS and PDC are not affected by the same disasters?<br>2.Have any provision for alternate physical location of employees been made in case of non-availability of the primary site Disaster Recovery?<br>Does the organisation have suitable provisions for Books and records backup and recovery (hard copy and electronic)?<br>Have all mission-critical systems been identified and provision for backup for such systems been made? |
| **9** | **Segregation of Data and Processing facilities** |
| 9(a) | The system auditor should check and comment on the segregation of data and processing facilities at the Depository Participant in case the Depository Participant is also running other businesses. |
| 9(b) | System Auditor to check where the Depository Participant having more than one entity within a group or having common Promoters or where both Holding/subsidiary entities are registered as Depository Participant has maintained appropriate segregation of infrastructure and data to uphold confidentiality. |
| **10** | **Back-office data** |
| 10(a) | Data consistency -The system auditor should verify whether aggregate back office data of the<br>Depository Participant matches with the data submitted / available with the Depository through online data view / download provided by Depository to Depository Participants. |
| 10(b) | Trail Logs - The system auditor should specifically comment on the logs of back office data to ascertain whether editing or deletion of records have been properly documented and recorded and does not result in any irregularities. |
| **11** | **User Management** |
| 11(a) | User Management Policy - The system auditor should check whether the Depository Participant has a well documented policy that provides for user management and that the user management policy explicitly defines user, database, and application access matrix. |

| Audit TOR Clause | TOR Status |
|---|---|
| 11(b) | Access to Authorized users -The system auditor should check whether the system allows access only to the authorized users of the depository systems. Whether there is a proper documentation of the authorized users in the form of user application approval, copies of user qualification and other necessary documents. |
| 11(c) | User Creation / Deletion - The system auditor should check whether new user ids were created / deleted as per user management policy and whether the user ids are unique in nature. |
| 11(d) | User Disablement – The system auditor should check whether non-complaint users are disabled and appropriate logs (such as event log of the user) are maintained. |
| 11(e) | User Management system: User Deletion: Users are deleted as per the Depository guidelines Reissue of User Ids: User Ids are reissued as per the Depository guidelines. Locked User Accounts: Users whose accounts are locked are unlocked only after documented unlocking requests are made and deactivate dormant account/users. |
| 11(f) | Is there any process to control the installation of approved software on endpoints. Has member implemented measures to control usage of VBA/macros in office documents, control permissible attachment types in email systems . |
| **12** | **IT Infrastructure Management ( including use of various Cloud computing models such as Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS))** |
| 12(a) | IT Governance and Policy – The system auditor should verify whether the relevant IT Infrastructure-related policies and standards exist and are regularly reviewed and updated. Compliance with these policies is periodically assessed. |
| 12(b) | IT Infrastructure Planning – The system auditor should verify whether the plans/policy for the appropriate management and replacement of aging IT infrastructure components have been documented, approved, and implemented. The activities, schedules and resources needed to achieve objectives related to IT infrastructure have been integrated into business plans and budgets. |
| 12(c) | IT Infrastructure Availability (SLA Parameters) - The system auditor should verify whether the Depository Participant has a process in place to define its required availability of the IT infrastructure, and its tolerance to outages. In cases where there |

| Audit TOR Clause | TOR Status |
|---|---|
| | is huge reliance on vendors for the provision of IT services to the Depository Participant, the system auditor should also verify that the Mean Time To Recovery (MTTR) mentioned in the Service Level Agreement (SLA) by the service provider satisfies the requirements of the Depository Participant |
| 12(d) | IT Performance Monitoring (SLA Monitoring) - The system auditor should verify that the results of SLA performance monitoring are documented and are reported to the management of the Depository Participant. |
| 12(e) | Infrastructure High Availability<br>- Does the organization have a documented process for identifying single point of failure?<br>- Does the organization have a documented process for failover?<br>- Does the organization ensure that various components pertaining to networks, servers, storage have sufficient redundancy?<br>- Does the organization conduct periodic redundancy/contingency testing? |
| 12(f) | To ensure information security for the organization in general and the installed system in particular, policy and procedures must be established, implemented, and maintained. Does the organization's documented policy and procedures include the following policies and if so, whether they have been implemented by the organization: Information Security Policy Password Policy User Management and Access Control Policy Network Security Policy Application Software Policy Change Management Policy Backup Policy BCP Management Policy Audit Trail Policy Capacity Management Plan Does the organization follow any other policy or procedures or documented practices that are relevant. |
| 12(g) | Are documented practices available for various system processes<br>Day Begins<br>Day Ends<br>Other system processes<br>a) Audit Trails<br>b) Access Logs<br>c) Transaction Logs<br>d) Backup Logs<br>e) Alert Logs |

| Audit TOR Clause | TOR Status |
|---|---|
| | f) Activity Logs<br>g) Retention Period<br>h) Data Maintenance |
| 12(h) | In case of failure, is there an escalation procedure implemented?<br>Day Begin<br>Day End<br>Other system processes<br><br>Details of the various response procedures including for<br>a) Access Control failure<br>b) Day Begin failure<br>c) Day End failure<br>d) Other system Processes failure |
| 12(i) | Vulnerability Assessment, Penetration Testing & Application Security Assessments - Are periodic vulnerability assessments for all the critical assets including Servers, OS, Database, Middleware, Network Devices, Firewalls, IDS /IPS etc conducted? |
| 12(j) | Standards & Guidelines - Does the organization maintain standards and guidelines for information security related controls, applicable to various IT functions such as System Administration, Database Administration, Network, Application, and Middleware etc.? Does the organization maintain Hardening Standards pertaining to all the technologies deployed within the organization related to Applications, OS, Hardware, Software, Middleware, Database, Network Devices and Desktops? Does the organization have a process for deploying OS, Hardware, Software, Middleware, Database, Network Devices and Desktops after ensuring that they are free from vulnerabilities? Are the defined standards, guidelines updated and reviewed periodically? |
| 12(k) | Information Security Policy & Procedure - Does the organization's documented policy and procedures include the information security policy and if so are they compliant with legal and regulatory requirements? Are the defined policies & procedures reviewed on a periodic basis? |
| 12(l) | Information Security Policy & Procedure - Are any other standards/guidelines like ISO 27001 etc. being followed? Does the organization have an Information Security Forum |

| Audit TOR Clause | TOR Status |
|---|---|
| | to provide overall direction to information security initiatives based on business objectives? |
| 12(m) | Information Classification & Protection - Has the organization defined Systematic and documented framework for Information Classification & Protection? Are the information items classified and protected in accordance with business criticality and sensitivity in terms of Confidentiality, Integrity & Availability? Does the organization conduct periodic information classification process audits? Has the organization deployed suitable controls to prevent leakage of sensitive information? |
| 12(n) | Vulnerability Assessment, Penetration Testing & Application Security Assessments - Does the organization maintain an annual VAPT and Application Security Assessment activity calendar? Is periodic Router ACL review conducted as a part of Vulnerability Assessment? |
| 12(o) | Does the organisation have hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments. |
| 12(p) | Cloud Service Controls - Does the organization check public accessibility of all Cloud instances in use. Does the organization make sure that no server/bucket is inadvertently leaking data due to inappropriate configurations. |
| 12(q) | Does the organization ensure proper security of Cloud access tokens. Does the organization ensure that the tokens are not exposed publicly in website source code, any configuration files etc. |
| 12(r) | Does the organization implement appropriate security measures for production, testing, staging, and backup environments hosted on cloud. Does the organization ensure that production environment is kept properly segregated from these environments? Does the organization disable/remove older or testing environments if their usage is no longer required? |
| 12(s) | The Apache Software Foundation released an emergency patch as part of the 2.15.0 release of Log4j that fixes the Remote Code Execution (RCE) vulnerability. Does the Organizations verify the use of the latest and stable version of Log4j package in their environment or any third parties component engaged with them through scanning and patching of such vulnerabilities? |

| Audit TOR Clause | TOR Status |
|---|---|
| 12(t) | Has the Depository Participant obtained and maintained valid SOC-II compliance reports from all third-party vendors providing virtual assets (e.g., cloud services such as SaaS, PaaS, IaaS)? |
| **13** | **Software Testing Procedures - The system auditor should check whether the Depository Participant has complied with the guidelines and instructions of SEBI with regard to testing of software and new patches, including the following:** |
| 13(a) | Test Procedure Review – The system auditor should review and evaluate the procedures for system and software/program testing. The system auditor should also review the adequacy of tests. |
| 13(b) | Documentation – The system auditor should verify whether the documentation related to testing procedures, test data, and resulting output were adequate and follow the organizations standards. |
| 13(c) | Test Cases – The system auditor should review the internal test cases and comment upon the adequacy of the same with respect to the requirements of the various SEBI circulars. |
| **14** | **Additional Points** |
| 14(a) | Antivirus Management - Does the organization have a documented process/procedure for Antivirus Management? Are all information assets protected with anti-virus software and the latest anti-virus signature updates? Does the organization periodically performs scans for virus/malicious code on computing resources, email, internet and other traffic at the Network Gateway/entry points in the IT Infrastructure? Does the organization have a documented process/procedure for tracking, reporting and responding to virus related incidents? |
| 14(b) | Anti-virus - Is a malicious code protection system implemented? If Yes, then Are the definition files up-to-date? Any instances of infection? Last date of virus check of entire system |
| 14(c) | The installed system provides a system based event logging and system monitoring facility which monitors and logs all activities / events arising from actions taken on the gateway / database server, authorized user terminal and transactions processed for clients or otherwise and the same is not susceptible to manipulation. The installed systems has a provision for On-line surveillance and risk management as per the SEBI |

| Audit TOR Clause | TOR Status |
|---|---|
| | guidelines and includes - Number of users logged in / hooked on to the network including privileges of each user. The installed systems has a provision for off line monitoring and risk management and includes reports / logs on: a) Number of authorized users b) Activity logs c) Systems logs d) Number of active clients |
| 14(d) | Insurance - The insurance policy of the Member covers the additional risk of usage of system and probable losses in case of software malfunction |
| 14(e) | Firewall - Whether suitable firewalls are implemented. Are the rules defined in the firewall adequate to prevent unauthorized access to depository systems |
| 14(f) | Compliance - Does the organization have a documented process/policy implemented to ensure compliance with legal, statutory, regulatory, and contractual obligations and avoid compliance breaches. Does the organization ensure compliance to the following. · IT Act 2000 · SEBI Requirements Does the organization maintain an integrated compliance checklist. Are these defined checklists periodically updated and reviewed to incorporate changes in rules, regulations, or compliance requirements. Are the servers of depository applications and back office located in India. |
| 14(g) | Vendor Certified Network Diagram Date of submission of network diagram to Depository (Only in case of change in network setup, member needs to submit revised scanned copy network diagram along with this report) Verify number of nodes in diagram with actual Verify location(s) of nodes in the network |
| 14(h) | DOS - Has the organization implemented strong monitoring, logging, detection and analysis capability to detect and mitigate DOS/DDOS attacks? Does the organization have a documented process/procedure/policy defining roles and responsibilities and plan of action in order to deal with DOS/DDOS attacks pro-actively and post the incidence? |
| 14(i) | DOS - Does the organization periodically conduct mock DOS scenarios to have insight into the preparedness in tackling with DOS/DDOS attacks? |
| 14(j) | Third Party Information Security Management - Does the organization have a documented process/framework for Third Party Vendor Management including at a minimum process and procedure for on-boarding/off-boarding of vendors, checklist for prescribing and assessing compliance, assessment and audit for both onsite & offsite vendors? Does the organization conducts periodic information security compliance audits/reviews for both onsite and offsite vendors? Are Risks associated with |

| Audit TOR Clause | TOR Status |
|---|---|
| | employing third party vendors addressed and mitigated? Is the defined process/framework periodically reviewed? |
| 14(k) | Capacity Management - Does the organization have documented processes/procedures for capacity management for all the IT assets. |
| 14(l) | Independent Audits - Are periodic independent audits conducted by Third Party / internal Auditors? Are the audit findings tracked to closure? |
| 14(m) | Human Resources Security, Acceptable Usage & Awareness Trainings - Are periodic surprise audits and social engineering attacks conducted to assess security awareness of employees and vendors? Has the organization implemented policy/procedure defining appropriate use of information assets provided to employees and vendors in order to protect these assets from inappropriate use? Are these policies/procedures periodically reviewed and updated? Does the organization perform Background Checks for employees (permanent, temporary) before employment? Does the organization conduct Information Security Awareness Program through trainings and Quiz for employees and vendors? |
| **15** | **AI-ML** |
| 15(a) | Are adequate safeguards in place to prevent abnormal behaviour of the AI or ML application / System. |
| 15(b) | Has the Depository Participant reported details of applications or systems using AI/ML to Depository on an annual basis in accordance with SEBI circular SEBI/HO/MIRSD/DOS2/CIR/P/2019/10 dated January 04, 2019 and subsequent amendments made thereto along with the circulars/communiques issued by the Depository. |
| 15(c) | Whether AI / ML systems comply for all above System Audit Checklist points. In case of any observation, please report. |
| **16** | **Asset Management** |
| 16(a) | Does the organization have a documented process/framework for managing all the hardware & software assets? Does the organization maintain a centralized asset repository? Are periodic reconciliation audits conducted for all the hardware and software assets to confirm compliance to licensing requirements and asset inventory? Has the member maintained a list of approved/ authorised software? Whether the IT |

| Audit TOR Clause | TOR Status |
|---|---|
| | asset inventory contains the information regarding the hostname, IP Address, Asset Owner, Operating System details, Criticality of asset, Asset Tagging, end-of-life/ end-of-support, last patched date, etc. Whether the mitigating / compensatory controls mentioned in Risk Register are adequate to address the risks emanating from End of Life or End of Support Software / Systems? Whether the installed Software Versions and License are reviewed and Risk related to Software has been addressed in Risk Register? |
| **17** | **Phishing & Malware Protection** |
| 17(a) | Has the organization implemented controls/ mechanism to identify and respond to phishing attempts on their critical websites?<br>Are the organizations websites monitored for Phishing & Malware attacks?<br>Does the organization have a process for tracking down phishing sites? |
| **18** | **Remote Access Controls** |
| 18(a) | Does the organization have proper remote access policy framework incorporating the specific requirements of accessing the enterprise resources are securely located in the data center from home, using internet connection? |
| 18(b) | For implementation of the concept of trusted machine as end users: Does the organization have categorized the machines as official desktops / laptops and accordingly the same are configured to ensure implementation of solution stack considering the requirements of authorized access? |
| 18(c) | Does the organizations Official devices have appropriate security measures to ensure that the configuration is not tampered with. Does the organization ensure that internet connectivity provided on all official are not getting used for any purpose other than the use of remote access to data center resources?. |
| 18(d) | Does the organization ensure that If personal devices (BYOD) are allowed for general functions, then appropriate guidelines are issued to indicate positive and negative list of applications that are permitted on such devices?. Further, these devices are subject to periodic audit? |
| 18(e) | Does the organization implement various measures related to Multi-Factor Authentication (MFA) for verification of user access so as to ensure better data confidentiality and accessibility.? VPN remote access through MFA also needs be implemented. |

| Audit TOR Clause | TOR Status |
|---|---|
| 18(f) | Does the organization ensure that only trusted machine are permitted to access the data center resources? .Does the organizations Virtual Private Network (VPN) remote login is device specific through the binding of the Media Access Control (MAC) address of the device with the IP address to implement appropriate security control measures?. |
| 18(g) | Does the organization have appropriate risk mitigation mechanisms whenever remote access of data center resources is permitted for service providers?. |
| 18(h) | For on-site monitoring, the Member, Does the organization implement adequate safeguard mechanisms such as cameras, security guards, nearby co- workers to reinforce technological activities?. |
| 18(i) | Does the organizations backup, restore and archival functions work seamlessly, particularly if the users have remote access to internal systems.? |
| 18(j) | Does the organization apply only necessary and applicable pathches to the existing hardware and software? |
| 18(k) | Does the organization analyse generated alerts and alarms? And take appropriate decisions to address the security concerns?.Are the organizations security controls for the Remote Access requirements integrated with the SOC Engine and part of the overall monitoring of the security posture? |
| 18(l) | Does the organization have updated the incident response plan in view of the current pandemic? Does the plan cover following: 1.Increase awareness of information technology support mechanisms for employees who work remotely. 2.Implement cyber security advisories received from SEBI, Depository, CERT-IN and NCIIPC on a regular basis. 3.Further, all the guidelines developed and implemented during pandemic situation shall become SOPs post Covid-19 situation for future preparedness. 4. Disable use of Macros in Microsoft Office |
| **19** | **SEBI and Depository Compliances** |
| 19(a) | Auditor to list all applicable Circulars, Notices, Guidelines, and advisories published by SEBI and Depository. |
| 19(b) | 1- Adherence to all such Circulars, Notices, Guidelines, and advisories published |
| 19(c) | 2- Reporting adherences based on prescribed periodicity in point 1 above |

| Audit TOR Clause | TOR Status |
|---|---|
| 19(d) | Has Member taken corrective steps to rectify the deficiencies observed in the inspection carried out by SEBI? Further, whether Member has complied with the qualifications/violations made in last SEBI inspection report? |
| 19(e) | Has Member taken corrective steps to rectify the deficiencies observed in the inspection carried out by Depository? Further, has Member complied with the qualifications/violations made in last Depository inspection report? |
| **20** | **TECHNICAL GLITCH** |
| 20(a) | Member has reported all instances of technical glitches within the prescribed timelines during the audit period in accordance with regulatory guidelines. Member has correctly reported the issues faced and duration of the downtime. Member has implemented all the measures as mentioned in RCAs and has taken necessary steps to prevent the recurrence of such technical glitch. |
| 20(b) | Does the organisation have internal policy to handle technical glitches in accordance with the framework defined in circular. |
| 20(c) | Does the policy cover following ? 1. Outline the key systems/departments handling the normal function /operation of the Member and assign responsibilities at business owner and technology owner level. 2. Lay down the processes/steps to be adopted in case of technical glitches along with the timelines and communication with concerned stakeholders including clients. 3. Define the Escalation matrix including reporting of such incident to the Depository. |
| 20(d) | Whether the Depository Participant has implemented the measures such as Change Management and Patch Management and the recommended measures as per RCA and taken steps to prevent its recurrence. The System Auditor should review the implemented measures. |
| 20(e) | Does the Member monitor the peak load of their critical systems—including servers and network architecture—and determine the peak load based on the highest peak observed during the relevant period (a calendar quarter for QSBs, a calendar half-year for specified members, and a calendar year for other members). |