Central Depository Services (India) Limited

Convenient ⌖ Dependable ⌖ Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

CDSL/A,I&C/DP/POLCY/2023/298 **May 16, 2023**

SUBMISSION OF ANNUAL SYSTEM AUDIT REPORT

Depository Participants (DPs) are advised to refer to Communique no. CDSL/A,I&C/DP/POLCY/2022/298 dated May 31, 2022, on submission of annual system audit report and providing there with manual for submission of the report.

Further, as per the requirements specified under SEBI Circular no. SEBI/HO/MIRSD/TPD/P/CIR/ 2022/80 dated June 07, 2022 (Communique no. CDSL/OPS/DP/POLCY/ 2022/323 dated June 09, 2022) the checklist for submission of the repot has been modified (enclosed as Annexure I - with track changes and Annexure II - without track changes respectively). In terms of para 3 of the above-mentioned SEBI Circular DPs are required to submit a declaration from their MD/ CEO/ Partners/ Proprietors certifying compliance by them with all SEBI Circulars and advisories related to Cyber security from time to time, along with the Annual System Audit Report.

DPs are required to ensure compliance by submitting the system audit report as per the schedule given below:

Report	Periodicity / Frequency	Due date of submission
Annual System Audit Report (Cyber Security Annual Report)	Annually (Online submission on https://auditweb.cdslindia.com. For user manual, refer Communique DP2021-445)	Within three months of the end of the financial year. i.e. by 30th June.

Queries, if any, regarding this Communiqué may be addressed to CDSL-Audit on (022) 2305 8515 / 2305 8679 / 2305 8678 / 2305 8519 / 2305 8520.

sd/-

Ajit Prabhu
Sr. Manager – Audit, Inspection & Compliance

KEYWORD : Audit

Annexure I

Audit TOR Clause	Checkpoints Description
1	**Governance**
1(a)	Whether the Participant has formulated a comprehensive Cyber Security and Cyber Resilience policy document encompassing the framework mentioned in the circular? In case of deviations from the suggested framework, whether reasons for such deviations, technical or otherwise, areprovided in the policy document? Is the policy document approved by theBoard / Partners / Proprietor of the organization? Is the policy reviewed periodically or atleast on annual basis?
1(b)	Whether the Cyber Security Policy includesthe following process to identify, assess, and manage Cyber Security risk associated with processes, information, networks and systems: a. 'Identify' critical IT assets and risks associated with such assets. b. 'Protect' assets by deploying suitable controls, tools and measures. c. 'Detect' incidents, anomalies and attacks through appropriate monitoring tools/processes. d. 'Respond' by taking immediate steps after identification of the incident, anomaly or attack. e. 'Recover' from incident through incident management and other appropriate recovery mechanisms.
1(c)	Whether the Cyber Security Policy of Participants has considered the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organization (NTRO), Government of India (titled 'Guidelines for Protection of National Critical Information Infrastructure') and subsequent revisions, if any, from time to time?
1(d)	Whether Participant refers to best practices from international standards like ISO 27001, COBIT 5, etc., or theirsubsequent revisions, if any, from time to time?
1(e)	Whether Participant has designated a senior official or management personnel (henceforth, referred to as the "Designated Officer") whose function would be to assess, identify, and reduce security and Cyber Security risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation ofprocesses and procedures as per the Cyber Security Policy?
1(f)	Whether the Board / Partners / Proprietor of the Participant haveformed an internal Technology Committee comprising of experts?
1(g)	Whether the Participant has established a reporting procedure to facilitate communication of unusual activities andevents to the Designated Officer in a timely

	manner?
1(h)	Does the "Technology Committee" along with designated officer reviews the status of implementation of Cyber Security & Cyber Resilience Policy on half yearly basis and same has been placed before the Board / Partners / Proprietor of the Participant?
1(i)	Does the designated officer andtechnology committee periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen Cyber Security andcyber resilience framework?
1(j)	Whether Participant has defined and documented the responsibilities of its employees, outsourced staff, and employees of vendors, members or participants and other entities, who may have privileged access or use systems / networks of the Participant towards ensuring the goal of Cyber Security?
2	**Identification**
~~2(a)~~	~~Whether Participant has identified critical assets based on their sensitivity and criticality for business operations, services and data management and maintained up-to-date inventory of its hardware and systems and the personnel to whom these have been issued, software andinformation assets (internal and external), details of its network resources, connections to its network and data flows?~~
2(a)	Whether Participant has identified critical assets based on their sensitivity and criticality for business operations, services and data management. The critical assets shall include business critical systems, internet facing applications /systems, systems that contain sensitive data, sensitive personal data, sensitive financial data, Personally Identifiable Information (PII) data, etc. All the ancillary systems used for accessing/communicating with critical systems either for operations or maintenance shall also be classified as critical system.
2 (b)	Whether Participants have approved the list of critical systems from their Board/Partners/Proprietor
2 (c)	Whether Participants have maintain up-to-date inventory of its hardware and systems, software and information assets (internal and external), details of its network resources, connections to its network and data flows
2(d)	Whether Participant has identified cyberrisks (threats and vulnerabilities) that it may face, along with the likelihood of suchthreats and impact on the business andthereby, deploy controls commensurate to the criticality?
3	**Protection**
I	**Access Control**
3(a)	Any access to Participants' systems, applications, networks, databases, etc., should be for a defined purpose andfor a defined period. Whether Participant has granted access to IT systems, applications, databases and networks on a need-to-use basis and based on the principle of least privilege and has been granted for the period

	when the access is required and has been authorized using strong authentication mechanisms?
3(b)	Whether Participant has implemented an access policy which addresses strong password controls for users' access to systems, applications, networks and databases?(Illustrative examples for this are given in Annexure C of SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018)
3(c)	Whether all critical systems of the Participant accessible over the internet have two-factor security (such as VPNs, Firewall controls etc.)?
3(d)	Whether Participant has ensured that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes and such logs have been maintained and stored in a secure location for a time period not less than two (2) years?
3(e)	Whether Participant has deployed controls and security measures tosupervise staff with elevated system access entitlements (such as admin or privileged users) to Participant's critical systems and controls and measures inter- alia includes restricting the number of privileged users, periodic review of privileged users' activities, disallow privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.?
3(f)	Whether employees and outsourced staff such as employees of vendors or service providers, who may have been given authorized access to the Participants' critical systems, networks and othercomputer resources, have been subjected to stringent supervision, monitoring and access restrictions?
3(g)	Whether Participant has formulated an Internet access policy to monitor andregulate the use of internet and internet-based services such as social media sites, cloud-based internet storage sites, etc. within the Participant's critical IT infrastructure?
3(h)	Whether User Management addresses deactivation of access of privileges ofusers who are leaving the organization or whose access privileges have been withdrawn?
II	**Physical Security**
3(i)	Whether physical access to the critical systems has been restricted to minimum and only to authorized officials and physical access of outsourced staff/visitorsare properly supervised by ensuring at the minimum that outsourced staff/visitorsare accompanied at all times by authorized employees?
3(j)	Whether physical access to the critical systems is being revoked immediately, if the same is no longer required?
3(k)	Whether Participant has ensured that the perimeter of the critical equipmentroom, if any, are physically secured and monitored by employing physical,human and

	procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. where appropriate?
III	**Network Security Management**
3(l)	Whether Participant has established baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within their IT environment and the LAN and wireless networks are secured within the Participants' premises with proper access controls?
3(m)	Whether Participant has installed network security devices, such as firewalls, proxy servers, intrusion detection and prevention systems (IDS) to protect their IT infrastructure which is exposed to the internet, from security exposures originating from internal and external sources?
3(n)	Whether adequate controls have been deployed to address virus / malware / ransomware attacks. These controls may include host / network / application-based IDS systems, customized kernels for Linux, anti-virus and anti-malware software etc.
IV	**Data Security**
3(o)	Whether critical data has been identified and encrypted in motion and at rest by using strong encryption methods? (Illustrative measures in this regard are given in Annexure A and B of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018)
3(p)	Whether Participants has implemented measures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity and ensured that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties? (Illustrative measures to ensure security during transportation of data over the internet are given in Annexure B of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018)
3(q)	Whether the information security policy covers use of devices such as mobile phones, faxes, photocopiers, scanners, etc., within their critical IT infrastructure, that can be used for capturing and transmission of sensitive data? (For instance, defining access policies for personnel, and network connectivity for such devices etc.)
3(r)	Whether Participant allows only authorized data storage devices within their IT infrastructure through appropriate validation processes?
3(s)	Whether Participant deploys only hardened hardware / software, including replacing default passwords with strong passwords and disabling or removing services identified as unnecessary for the functioning of the system?
3(t)	Whether open ports on networks and systems which are not in use or that can be potentially used for exploitation of data, have been blocked and measures have been

	taken to secure them?
V	**Application Security in Customer Facing Applications**
3(u)	Whether application security is in place for Customer facing applications offeredover the Internet such as IBTs (Internet Based Trading applications), portals containing sensitive or private information and Back office applications (repository of financial and personal information offered by Participants to Customers) as they carry significant attack surfaces by virtue of being available publicly over the Internet for mass use? (An illustrative list of measures forensuring security in such applications isprovided in Annexure C of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018)
VI	**Certification of off-the-shelf products**
3(v)	Whether Participant has ensured that off the shelf products being used for core business functionality (such as Back office applications) bears Indian Common criteria certification of Evaluation Assurance Level 4which is being provided by Standardisation Testing and Quality Certification (STQC) (Ministry of Electronics and InformationTechnology)(except Custom developed / in-house software and components need not obtain the certification, but have to undergo intensive regression testing, configuration testing etc. The scope of tests should include business logic and security controls)?
VII	**Patch management**
3(w)	Whether Participants has established and ensure that the patch management procedures includes the identification, categorization and prioritization of patches and updates and the implementation timeframe for each category of patches has been established to apply them in a timely manner?
3(x)	Whether Participant has performed rigorous testing of security patches and updates, where possible, before deployment into the production environment so as to ensure that the application of patches do not impact othersystems?
VIII	**Disposal of data, systems and storage Devices**
3(y)	Whether Participant has framed suitable policy for disposal of storage media and systems and the critical data / Information on such devices and systems has been removed by using methods such as crypto shredding/degauss / Physical destruction as applicable?
3(z)	Whether Participant has formulated a data-disposal and data- retention policy to identify the value and lifetime of various parcels of data?
IX	**Vulnerability Assessment and PenetrationTesting (VAPT)**
~~3(aa)~~	~~Whether Participant regularly conductsvulnerability assessment to detect security~~

	~~vulnerabilities in their IT environments exposed to the internet?~~
3(aa)	Whether Participant conduct periodic Vulnerability Assessment and Penetration Tests (VAPT) at least once in a financial year which inter-alia include critical assets and infrastructure components like Servers, Networking systems, Security devices, load balancers, other IT systems pertaining to the activities done as Participants etc., in order to detect security vulnerabilities in the IT environment and in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks.
3(ab)	Whether Participants have engaged CERT-In empaneled organizations for conducting VAPT and submitted final report of VAPT to Depository after approval from Technology Committee of Participants, within 1 month of completion of VAPT activity
3(ac)	Whether Participants have performed vulnerability scanning and conduct penetration testing prior to the commissioning of a new system which is a critical system or part of an existing critical system.
3(ad)	Whether Participants have remedied all findings of VAPT on immediate basis and compliance of closure of findings of VAPT submitted to Depository within 3 months post the submission of final VAPT report.
~~3(ab)~~	~~Whether Participant with systems publicly available over the internet has carried out penetration tests, at-least once a year, in order to conduct an in-depth evaluation of the security posture of the system throughsimulations of actual attacks on itssystems and networks that are exposed to theinternet?~~ ~~In addition, whether Participant hasperformed vulnerability scanning and conducted penetration testing prior to the commissioning of a new system that is accessible over the internet?~~
3(ae)	In case of vulnerabilities discovered in off- the-shelf products (used for core business) or applications provided by vendors, whether Participant has reported them to the vendors and CDSL in a timely manner?
~~3(ad)~~	~~Whether remedial actions have been immediately taken to address gaps that are identified during vulnerability assessment and penetration testing?~~
4	**Monitoring and Detection**
4(a)	Whether Participant has established appropriate security monitoring systems and processes to facilitate continuous monitoring of security events / alerts and timely detection of unauthorised or malicious activities, unauthorised changes, unauthorised access and unauthorised copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties and the security logs of systems, applications and network devices exposed to the internet has been monitored for anomalies?
4(b)	Further, to ensure high resilience, high availability and timely detection of attacks on

	systems and networks exposed to the internet, whether Participant has implemented suitable mechanisms tomonitor capacity utilization of its criticalsystems and networks that are exposed to the internet, for example, controls such as firewalls to monitor bandwidth usage?
5	**Response and Recovery**
5(a)	Whether alerts generated from monitoring and detection systems have been suitably investigated in order to determine activities that are to be performed to prevent expansion of such incident of cyber attack or breach, mitigate its effect and eradicate the incident?
5(b)	Whether the response and recovery plan of the Participant includes plans for the timely restoration of systems affected by incidents of cyber-attacks or breaches, for instance, offering alternate services or systems to Customers and has same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) asspecified by SEBI for Market Infrastructure Institutions vide SEBI circular CIR/MRD/DMS/17/20 dated June 22, 2012as amended from time to time?
5(c)	Whether the response plan defines responsibilities and actions to be performed by its employees and support / outsourced staff in the event of cyber-attacks or breach of Cyber Security mechanism?
5(d)	Whether any incident of loss or destruction of data or systems have been thoroughly analyzed and lessons learned from such incidents have been incorporated to strengthen the security mechanism and improve recovery planning and processes?
5(e)	Whether Participant has conducted suitable periodic drills to test the adequacy and effectiveness of theaforementioned response and recoveryplan?
6	**Sharing of Information**
6(a)	Whether quarterly reports containing information on cyber-attacks and threats experienced by Participant and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs/ vulnerabilities / threats that may be useful for other Participants have been submitted to CDSL?
7	**Training and Education**
7(a)	Whether Participant has worked onbuilding Cyber Security and basic system hygiene awareness of staff (with a focus on staff from non-technical disciplines)?
7(b)	Whether Participant has conducted periodic training programs to enhanceknowledge of IT / Cyber Security Policy and standards among the employees incorporating up-to-date Cyber Security threat alerts and where possible, has extended to outsourced staff, vendors etc.?
7(c)	Whether the training programs have been reviewed and updated to ensurethat the contents of the program remain current and relevant?

8	**Systems managed by vendors**
8(a)	Where the systems (IBT, Back office and other Customer facing applications, IT infrastructure, etc.) of Participant are managed by vendors and the Participant is unable to implement some of the aforementioned guidelines directly, thewhether the Participant has instructed the vendors to adhere to the applicable guidelines in the Cyber Security and Cyber Resilience policy and obtain the necessary self-certifications from them to ensure compliance with the policy guidelines?
9	**AI/ML**
9(a)	Are adequate safeguards in place to prevent abnormal behaviour of the AI or ML application / System?
9(b)	Has Participant reported details of AI/ML to Depository on a quarterly basis in accordance with SEBI circular SEBI/HO/MI RSD/DOS2/ CIR/P/2019/ 10 dated January 04, 2019?
9(c)	Whether AI / ML systems comply for all above System Audit Checklist points. In case of any observation, please report?
10	**Additional Information about Participant**
10(a)	Whether any other deviation/non- compliance observed by auditor which is not specifically covered above?
10(b)	Whether any deviation/non- compliance observed during last audit?
10(c)	Status of compliance for deviations observed during last audit
11	**Data Leakage** **(New Point)**
11 (a)	Whether Participants have approved Data Leakage Policy
11 (b)	Whether Participants have approved Data Leakage Solution
11 (c)	Whether Participants have exception reporting and escalation mechanism in case of data breaches / data leaks
11 (d)	Whether Participants have reported incidents related to data breaches / data leaks in timely manner to CERT-IN, SEBI and CDSL

Audit TOR Clause	Checkpoints Description
1	**Governance**
1(a)	Whether the Participant has formulated a comprehensive Cyber Security and Cyber Resilience policy document encompassing the framework mentioned in the circular? In case of deviations from the suggested framework, whether reasons for such deviations, technical or otherwise, areprovided in the policy document? Is the policy document approved by theBoard / Partners / Proprietor of the organization? Is the policy reviewed periodically or atleast on annual basis?
1(b)	Whether the Cyber Security Policy includesthe following process to identify, assess, and manage Cyber Security risk associated with processes, information, networks and systems: a. 'Identify' critical IT assets and risks associated with such assets. b. 'Protect' assets by deploying suitable controls, tools and measures. c. 'Detect' incidents, anomalies and attacks through appropriate monitoring tools/processes. d. 'Respond' by taking immediate steps after identification of the incident, anomaly or attack. e. 'Recover' from incident through incident management and other appropriate recovery mechanisms.
1(c)	Whether the Cyber Security Policy of Participants has considered the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organization (NTRO), Government of India (titled 'Guidelines for Protection of National Critical Information Infrastructure') and subsequent revisions, if any, from time to time?
1(d)	Whether Participant refers to best practices from international standards like ISO 27001, COBIT 5, etc., or theirsubsequent revisions, if any, from time to time?
1(e)	Whether Participant has designated a senior official or management personnel (henceforth, referred to as the "Designated Officer") whose function would be to assess, identify, and reduce security and Cyber Security risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation ofprocesses and procedures as per the Cyber Security Policy?
1(f)	Whether the Board / Partners / Proprietor of the Participant have formed an internal Technology Committee comprising of experts?

1(g)	Whether the Participant has established a reporting procedure to facilitate communication of unusual activities andevents to the Designated Officer in a timely manner?
1(h)	Does the "Technology Committee" along with designated officer reviews the status of implementation of Cyber Security & Cyber Resilience Policy on half yearly basis and same has been placed before the Board / Partners / Proprietor of the Participant?
1(i)	Does the designated officer andtechnology committee periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen Cyber Security andcyber resilience framework?
1(j)	Whether Participant has defined and documented the responsibilities of its employees, outsourced staff, and employees of vendors, members or participants and other entities, who may have privileged access or use systems / networks of the Participant towards ensuring the goal of Cyber Security?
2	**Identification**
2(a)	Whether Participant has identified critical assets based on their sensitivity and criticality for business operations, services and data management. The critical assets shall include business critical systems, internet facing applications /systems, systems that contain sensitive data, sensitive personal data, sensitive financial data, Personally Identifiable Information (PII) data, etc. All the ancillary systems used for accessing/communicating with critical systems either for operations or maintenance shall also be classified as critical system.
2 (b)	Whether Participants have approved the list of critical systems from their Board/Partners/Proprietor
2 (c)	Whether Participants have maintain up-to-date inventory of its hardware and systems, software and information assets (internal and external), details of its network resources, connections to its network and data flows
2(d)	Whether Participant has identified cyberrisks (threats and vulnerabilities) that it may face, along with the likelihood of suchthreats and impact on the business andthereby, deploy controls commensurate to the criticality?
3	**Protection**
I	**Access Control**
3(a)	Any access to Participants' systems, applications, networks, databases, etc., should be for a defined purpose andfor a defined period. Whether Participant has granted access to IT systems, applications, databases and networks on a need-to-use basis and based on the principle of least privilege and has been granted for the period

	when the access is required and has been authorized using strong authentication mechanisms?
3(b)	Whether Participant has implemented an access policy which addresses strong password controls for users' access to systems, applications, networks and databases?(Illustrative examples for this are given in Annexure C of SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018)
3(c)	Whether all critical systems of the Participant accessible over the internet have two-factor security (such as VPNs, Firewall controls etc.)?
3(d)	Whether Participant has ensured that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes and such logs have been maintained and stored in a secure location for a time period not less than two (2) years?
3(e)	Whether Participant has deployed controls and security measures tosupervise staff with elevated system access entitlements (such as admin or privileged users) to Participant's critical systems and controls and measures inter- alia includes restricting the number of privileged users, periodic review of privileged users' activities, disallow privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.?
3(f)	Whether employees and outsourced staff such as employees of vendors or service providers, who may have been given authorized access to the Participants' critical systems, networks and othercomputer resources, have been subjected to stringent supervision, monitoring and access restrictions?
3(g)	Whether Participant has formulated an Internet access policy to monitor andregulate the use of internet and internet-based services such as social media sites, cloud-based internet storage sites, etc. within the Participant's critical IT infrastructure?
3(h)	Whether User Management addresses deactivation of access of privileges ofusers who are leaving the organization or whose access privileges have been withdrawn?
II	**Physical Security**
3(i)	Whether physical access to the critical systems has been restricted to minimum and only to authorized officials and physical access of outsourced staff/visitorsare properly supervised by ensuring at the minimum that outsourced staff/visitorsare accompanied at all times by authorized employees?
3(j)	Whether physical access to the critical systems is being revoked immediately, if the same is no longer required?

3(k)	Whether Participant has ensured that the perimeter of the critical equipmentroom, if any, are physically secured and monitored by employing physical,human and procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. where appropriate?
III	**Network Security Management**
3(l)	Whether Participant has established baseline standards to facilitateconsistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within their IT environment and the LAN and wireless networks are secured within the Participants' premises with proper access controls?
3(m)	Whether Participant has installednetwork security devices, such as firewalls, proxy servers, intrusion detection and prevention systems (IDS) to protect their IT infrastructure which is exposed to the internet, from security exposures originating from internal and external sources?
3(n)	Whether adequate controls have been deployed to address virus / malware / ransomware attacks. These controls mayinclude host / network / application-based IDS systems, customized kernels forLinux, anti-virus and anti-malware software etc.
IV	**Data Security**
3(o)	Whether critical data has been identifiedand encrypted in motion and at rest byusing strong encryption methods? (Illustrative measures in this regard aregiven in Annexure A and B of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018)
3(p)	Whether Participants has implementedmeasures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity and ensured thatconfidentiality of information is not compromised during the process of exchanging and transferring information with external parties? (Illustrative measures to ensure security during transportation of data over the internet are given in Annexure B of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018)
3(q)	Whether the information security policy covers use of devices such as mobile phones, faxes, photocopiers, scanners, etc., within their critical IT infrastructure, that can be used for capturing and transmission of sensitive data? (For instance, defining access policies forpersonnel, and network connectivity for such devices etc.)
3(r)	Whether Participant allows only authorized data storage devices within their IT infrastructure through appropriate validation processes?

3(s)	Whether Participant deploys only hardened hardware / software, including replacing default passwords with strong passwords and disabling or removing services identified as unnecessary for the functioning of the system?
3(t)	Whether open ports on networks and systems which are not in use or that can be potentially used for exploitation of data, have been blocked and measures have been taken to secure them?
V	**Application Security in Customer Facing Applications**
3(u)	Whether application security is in place for Customer facing applications offeredover the Internet such as IBTs (Internet Based Trading applications), portals containing sensitive or private information and Back office applications (repository of financial and personal information offered by Participants to Customers) as they carry significant attack surfaces by virtue of being available publicly over the Internet for mass use? (An illustrative list of measures forensuring security in such applications isprovided in Annexure C of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018)
VI	**Certification of off-the-shelf products**
3(v)	Whether Participant has ensured that off the shelf products being used for core business functionality (such as Back office applications) bears Indian Common criteria certification of Evaluation Assurance Level 4which is being provided by Standardisation Testing and Quality Certification (STQC) (Ministry of Electronics and InformationTechnology)(except Custom developed / in-house software and components need not obtain the certification, but have to undergo intensive regression testing, configuration testing etc. The scope of tests should include business logic and security controls)?
VII	**Patch management**
3(w)	Whether Participants has established and ensure that the patch management procedures includes the identification, categorization and prioritization of patches and updates and the implementation timeframe for each category of patches has been established to apply them in a timely manner?
3(x)	Whether Participant has performed rigorous testing of security patches and updates, where possible, before deployment into the production environment so as to ensure that the application of patches do not impact othersystems?
VIII	**Disposal of data, systems and storage Devices**

3(y)	Whether Participant has framed suitable policy for disposal of storage media and systems and the critical data / Information on such devices and systems has been removed by using methods such as crypto shredding/degauss / Physical destruction as applicable?
3(z)	Whether Participant has formulated a data-disposal and data- retention policy to identify the value and lifetime of various parcels of data?
IX	**Vulnerability Assessment and PenetrationTesting (VAPT)**
3(aa)	Whether Participant conduct periodic Vulnerability Assessment and Penetration Tests (VAPT) at least once in a financial year which inter-alia include critical assets and infrastructure components like Servers, Networking systems, Security devices, load balancers, other IT systems pertaining to the activities done as Participants etc., in order to detect security vulnerabilities in the IT environment and in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks.
3(ab)	Whether Participants have engaged CERT-In empaneled organizations for conducting VAPT and submitted final report of VAPT to Depository after approval from Technology Committee of Participants, within 1 month of completion of VAPT activity
3(ac)	Whether Participants have performed vulnerability scanning and conduct penetration testing prior to the commissioning of a new system which is a critical system or part of an existing critical system.
3(ad)	Whether Participants have remedied all findings of VAPT on immediate basis and compliance of closure of findings of VAPT submitted to Depository within 3 months post the submission of final VAPT report.
3(ae)	In case of vulnerabilities discovered in off- the-shelf products (used for core business) or applications provided by vendors, whether Participant has reported them to the vendors and CDSL in a timely manner?
4	**Monitoring and Detection**
4(a)	Whether Participant has established appropriate security monitoring systems and processes to facilitate continuous monitoring of security events / alerts and timely detection of unauthorised or malicious activities, unauthorised changes, unauthorised access and unauthorised copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties and the security logs of systems, applications and network devices exposed to the internet has been monitored for anomalies?
4(b)	Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks exposed to the internet, whether Participant has implemented

	suitable mechanisms tomonitor capacity utilization of its criticalsystems and networks that are exposed to the internet, for example, controls such as firewalls to monitor bandwidth usage?
5	**Response and Recovery**
5(a)	Whether alerts generated from monitoring and detection systems have been suitably investigated in order to determine activities that are to be performed to prevent expansion of such incident of cyber attack or breach, mitigate its effect and eradicate the incident?
5(b)	Whether the response and recovery plan of the Participant includes plans for the timely restoration of systems affected by incidents of cyber-attacks or breaches, for instance, offering alternate services or systems to Customers and has same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) asspecified by SEBI for Market Infrastructure Institutions vide SEBI circular CIR/MRD/DMS/17/20 dated June 22, 2012as amended from time to time?
5(c)	Whether the response plan defines responsibilities and actions to be performed by its employees and support / outsourced staff in the event of cyber-attacks or breach of Cyber Security mechanism?
5(d)	Whether any incident of loss or destruction of data or systems have been thoroughly analyzed and lessons learned from such incidents have been incorporated to strengthen the security mechanism and improve recovery planning and processes?
5(e)	Whether Participant has conducted suitable periodic drills to test the adequacy and effectiveness of theaforementioned response and recoveryplan?
6	**Sharing of Information**
6(a)	Whether quarterly reports containing information on cyber-attacks and threats experienced by Participant and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs/ vulnerabilities / threats that may be useful for other Participants have been submitted to CDSL?
7	**Training and Education**
7(a)	Whether Participant has worked onbuilding Cyber Security and basic system hygiene awareness of staff (with a focus on staff from non-technical disciplines)?
7(b)	Whether Participant has conducted periodic training programs to enhanceknowledge of IT / Cyber Security Policy and standards among the employees incorporating up-to-date Cyber Security threat alerts and where possible, has extended to outsourced staff, vendors etc.?

7(c)	Whether the training programs have been reviewed and updated to ensurethat the contents of the program remain current and relevant?
8	**Systems managed by vendors**
8(a)	Where the systems (IBT, Back office and other Customer facing applications, IT infrastructure, etc.) of Participant are managed by vendors and the Participant is unable to implement some of the aforementioned guidelines directly, thewhether the Participant has instructed the vendors to adhere to the applicable guidelines in the Cyber Security and Cyber Resilience policy and obtain the necessary self-certifications from them to ensure compliance with the policy guidelines?
9	**AI/ML**
9(a)	Are adequate safeguards in place to prevent abnormal behaviour of the AI or ML application / System?
9(b)	Has Participant reported details of AI/ML to Depository on a quarterly basis in accordance with SEBI circular SEBI/HO/MI RSD/DOS2/ CIR/P/2019/ 10 dated January 04, 2019?
9(c)	Whether AI / ML systems comply for all above System Audit Checklist points. In case of any observation, please report?
10	**Additional Information about Participant**
10(a)	Whether any other deviation/non- compliance observed by auditor which is not specifically covered above?
10(b)	Whether any deviation/non- compliance observed during last audit?
10(c)	Status of compliance for deviations observed during last audit
11	**Data Leakage** **(New Point)**
11 (a)	Whether Participants have approved Data Leakage Policy
11 (b)	Whether Participants have approved Data Leakage Solution
11 (c)	Whether Participants have exception reporting and escalation mechanism in case of data breaches / data leaks
11 (d)	Whether Participants have reported incidents related to data breaches / data leaks in timely manner to CERT-IN, SEBI and CDSL