Circular No.: NSDL/POLICY/2024/0133 September 18, 2024

Subject: Submission of Annual Cyber Audit Report.

Attention of Participants is invited to Circular No. **NSDL/POLICY/2022/083 dated June 13, 2022 in response to SEBI Circular No. SEBI/HO/MIRSD/TPD/P/CIR/2022/80** dated **June 07, 2022,** on 'Modification in Cyber Security and Cyber resilience framework for Stockbrokers / Depository Participants'.

As per Paragraph 3 of the abovementioned SEBI circular, the Participants were mandated to conduct a comprehensive cyber security audit at least once in a financial year.

At present, Participants are required to submit a consolidated report to NSDL to comply with the abovementioned circular. Pursuant to guidance received from SEBI, w.e.f. FY 2024-25, Participants shall be required to submit two separate reports, i.e. One for Cyber Security Audit and One for System Audit.

The qualification, criteria for selection and appointment of auditor for conducting cyber security audit is attached as **Annexure A.** The terms of reference for cyber security audit report is attached as **Annexure B.**

As per para 3 of abovementioned SEBI circular, Participants shall also submit a declaration from its MD/ CEO/ Partners/ Proprietors certifying compliance by Participants with all SEBI Circulars and advisories related to Cyber security from time to time, along with the Cyber Security Audit report.

All Participants are requested to take note of the periodicity and due date of submission 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**	**Action Taken Report (ATR) Submission (if applicable)**
Annual Cyber Security 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.

Additionally, Participants are hereby requested to take note of the following.

- For each instance of non-compliance reported, auditors must assign a risk rating of 'High', 'Medium', or 'Low'.
- Participants are advised to schedule the audit at such a time that the Cyber Security Audit report can be shared with the auditor conducting System Audit

The steps for uploading Cyber Security Audit report will be shared via a separate circular.

Enclosure

Annexure A – Auditor Selection Norms.

Annexure B – Scope and Terms of Reference (TOR) for Cyber Audit Report.

Participants are requested to take note of the above and ensure compliance with the updated requirements.

For any clarifications on the circular, kindly email at dpaudit@nsdl.com or call us on (022)69446886.

For and on behalf of

National Securities Depository Limited

AROCKIARAJ Date: 2024.09.18 07:45:38 +05'30'

Arockiaraj
Manager

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 28 of 'Internal Controls/Reporting to NSDL/SEBI' chapter of NSDL Master Circular for Participants
Networth Certificate and Audited Financial Statements (yearly)	October 31st	Through e-PASS	Para 20.7 of NSDL Master Circular for Participants on Internal Controls/Reporting to NSDL / SEBI chapter.

Annexure A

Auditor Selection Norms

1. The Audit shall be conducted by **CERT-In empaneled organization/ entity.**

2. The Auditor/Auditor firm can perform minimum of 3 successive audits of the Participant. However, such an auditor shall be eligible for reappointment after a cooling – off period of two years and the Auditor should not have been engaged over the last two years in any consulting engagement with any departments / units of the Participant.

3. Auditors must preferably have a minimum of 3 years of experience in IT audit of Banking and Financial services, preferably in the Securities Market. E.g. Stock exchanges, clearing houses, depositories, stockbrokers, depository participants, mutual funds, etc. The audit experience should have covered all the major areas mentioned under various cybersecurity frameworks and guidelines issued by SEBI from time to time.

4. It is recommended that resources employed shall have relevant industry recognized certifications e.g. CISA (Certified information Systems Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, GSNA (GIAC Systems and Network Auditor), CISSP (Certified Information Systems Security professional) from International Information systems Security Certification Consortium, commonly known as (ISC)2.

5. The Auditor, as being appointed by Participants must **not have any conflict of interest** in conducting fair, objective, and independent audit. Further, the directors / partners of Audit firm shall not be related to any Directors/Promoters/Proprietor of the said Participants either directly or indirectly.

6. The Auditor shall not have any cases pending against its previous audited companies/firms, which fall under SEBI's jurisdiction, which point to its incompetence and/or unsuitability to perform the audit task.

7. The Participants and auditors 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.

Annexure B

Scope

The scope of cyber audit of Participants should cover all the systems i.e. systems and applications provided by Depositories to Participants as well as Participants own system whether in house or off the shelf products etc.

Terms of Reference (TOR) for Cyber Security Audit Report

Cyber Audit TOR Clause	Checkpoints Description
1	**Governance**
1(a)	Has the Depository Participant formulated a comprehensive Cyber Security and Cyber Resilience policy document encompassing the framework mentioned in the SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 and subsequent amendments made thereto.
1(b)	In case of deviations from the suggested framework, whether reasons for such deviations, technical or otherwise, are provided in the policy document.
1(c)	Is the policy document approved by the Board/ Partners/ Proprietor of the Depository Participant.
1(d)	Is the policy document reviewed by the Board/ Partners/ Proprietor of the Depository Participant at least annually with the view to strengthen and improve its Cyber Security and Cyber Resilience framework.
1(e)	Whether the Cyber Security Policy includes the 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.

Cyber Audit TOR Clause	Checkpoints Description
1(f)	Whether policy/ procedure document refers to best practices from international standards like ISO 27001, COBIT 5, etc., or their subsequent revisions, if any, from time to time.
1(g)	Has the policy document 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(h)	Has the Depository Participant designated a senior official or management personnel as 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 of processes and procedures as per the Cyber Security policy.
1(i)	Has the Depository Participant constituted a Technology Committee comprising of experts.
1(j)	Whether the Technology Committee has reviewed on a half yearly basis the implementation of the Cyber Security and Cyber Resilience policy, which includes:
	a) review of their current IT and Cyber Security and Cyber Resilience capabilities.
	b) setting goals for a target level of Cyber Resilience and establishing plans to improve and strengthen Cyber Security and Cyber Resilience.
	c) placing of the review report before the Board / Partners/ Proprietor of the Depository Participant for appropriate action.
1(k)	Whether the Designated Officer and the Technology Committee have periodically reviewed instances of cyber-attacks, if any, domestically and globally, and taken steps to strengthen Cyber Security and Cyber Resilience framework.
1(l)	Has the Depository Participant established a reporting procedure to facilitate communication of unusual activities and events to the Designated Officer in a timely manner.
1(m)	Has Depository Participant defined responsibilities of its employees, outsourced staff, and employees of vendors or participants and other entities, who may have privileged access or use systems/ networks of the Depository Participant towards ensuring the goal of Cyber Security.

Cyber Audit TOR Clause	Checkpoints Description
1(n)	Has the Depository Participant prepared detailed incident response plan. Has the Depository Participant defined roles and responsibilities of Chief Information Security Officer (CISO) and other senior personnel. Reporting and compliance requirements shall be clearly specified in the security policy. Whether the details of CISO are shared with CERT-In through Email (info@cert-in.org.in)
2	**Identification**
2(a)	Has the Depository Participant identified and classified critical assets based on their sensitivity and criticality for business operations, services and data management. Whether the critical assets 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. Whether all the ancillary systems used for accessing/communicating with critical systems either for operations or maintenance are also classified as critical systems. Has the Board/Partners/Proprietor of the Depository Participant approved the list of critical systems. Has the Depository Participant maintained up-to-date inventory of its hardware and systems and the personnel to whom these have been issued, software and information assets (internal and external), details of its network resources, connections to its network and data flows.
2(b)	Has the Depository Participant identified cyber risk or has the process to identify cyber risks (threats and vulnerabilities) that it may face, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.
3	**Protection**
3(a)	**Access controls** Whether the Depository Participant has a process to ensure that no person by virtue of rank or position has any intrinsic right to access confidential data, applications, system resources or facilities.

Cyber Audit TOR Clause	Checkpoints Description
3(b)	**Access controls** Whether any access to Depository Participant's systems, applications, networks, databases, etc., has a defined purpose and is for a defined period. Whether the Depository Participant grants access to IT systems, applications, databases, and networks on a need-to-use basis and the access is based on the principle of least privilege to provide security for both on-and off-premises resources (i.e., zero-trust models). Whether such access is granted for the period when the access is required and is authorized using strong authentication mechanisms. Whether maker-checker framework is implemented in strict manner and multi factor authentication (MFA) is enabled for all users that connect using online/internet facility and particularly for virtual private networks, webmail and user accounts that access critical systems and applications.
3(c)	Has the Depository Participant implemented an access policy which addresses strong password controls for users' access to systems, applications, networks, and databases. Whether the password policy includes clauses on: 1. Periodic review of accounts of ex-employees. 2. Reuse of password across multiple accounts. 3. Not storing the list of passwords on the system Illustrative examples for strong password controls are given in Annexure C of SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018
3(d)	Whether all critical systems of the Depository Participant accessible over the internet have two-factor security (such as VPNs, Firewall controls etc.)
3(e)	Whether the Depository Participant ensures that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes. Whether such logs are maintained and stored in a secure location for a time period not less than two (2) years. Has the Depository Participant implemented a strong log retention policy as per extant SEBI regulations and required by CERT-In and IT Act 2000. Has the Depository Participant audited all logs that are being collected.

Cyber Audit TOR Clause	Checkpoints Description
	Whether the Depository Participant monitors incidents to identify unusual patterns and behaviours.
3(f)	Whether the Depository Participant deploys controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users) to Depository Participant's critical systems. Whether such controls and measures inter-alia include 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. Whether maker-checker framework is implemented for modifying the user's right in internal applications.
3(g)	Whether the employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to the Depository Participant's critical systems, networks and other computer resources, are subject to stringent supervision, monitoring, and access restrictions.
3(h)	Whether the Depository Participant has formulated an Internet access policy to monitor and regulate the use of internet and internet-based services such as social media sites, cloud-based internet storage sites, etc. within the Depository Participant's critical IT infrastructure.
3(i)	Whether the User Management addresses the deactivation of access of privileges of users who are leaving the organization or whose access privileges have been withdrawn.
4	**Physical Security**
4(a)	Whether physical access to the critical systems is restricted to minimum and only to authorized officials. Whether physical access of outsourced staff/visitors is properly supervised by ensuring at the minimum that outsourced staff/visitors are always accompanied at all times by authorized employees.
4(b)	Whether physical access to the critical systems is revoked immediately if the same is no longer required.

Cyber Audit TOR Clause	Checkpoints Description
4(c)	Whether the Depository Participant ensures that the perimeter of the critical equipment's room, if any, is 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
5	**Network Security Management**
5(a)	Has the Depository Participant established baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within their IT environment.
5(b)	Whether the LAN and wireless networks are secured within the Depository Participant's premises with proper access controls.
5(c)	Whether the Depository Participant has installed network security devices, such as firewalls, proxy servers, intrusion detection and prevention systems (IDS) to protect its IT infrastructure which is exposed to the internet, from security exposures originating from internal and external sources.
5(d)	Whether adequate controls are 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.
5(e)	Whether the Depository Participant has deployed web and email filters on the network. Whether the Depository Participant has configured these devices to scan for known bad domains, sources, and addresses and block these before receiving and downloading messages. Whether the Depository Participant scans all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.
5(f)	Whether the Depository Participant blocks the malicious domains/IPs after diligently verifying them without impacting the operations. Whether CSIRT-Fin/CERT-In advisories which are published periodically referred for latest malicious domains/IPs, C&C DNS and links.

Cyber Audit TOR Clause	Checkpoints Description
5(g)	Whether the Depository Participant restricts execution of "PowerShell" and "wscript" in enterprise environment, if not required. Whether the Depository Participant ensures installation and use of the latest version of PowerShell, with enhanced logging enabled, script block logging and transcription enabled. Whether the Depository Participant sends the associated logs to a centralized log repository for monitoring and analysis.
5(h)	Whether the Depository Participant utilizes host-based firewall to prevent Remote Procedure Call (RPC) and Server Message Block (SMB) communication among endpoints whenever possible.
5(i)	Whether the Depository Participant implements the practice of whitelisting of ports based on business usage at Firewall level rather than blacklisting of certain ports. Whether the traffic on all other ports which have not been whitelisted is blocked by default.
6	**Data security**
6(a)	Whether critical/sensitive and Personally Identifiable Information (PII) data is identified, classified, 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
6(b)	Has the Depository Participant implemented measures to prevent unauthorized access or copying or transmission of data/ information held in contractual or fiduciary capacity. Whether it is 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
6(c)	Whether the information security policy also 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.
6(d)	Whether the Depository Participant allows only authorized data storage devices within their IT infrastructure through appropriate validation processes.

Cyber Audit TOR Clause	Checkpoints Description
6(e)	Whether the Depository Participant has enforced BYOD (Bring your own device) security policies, like requiring all devices to use a business-grade VPN service and antivirus protection.
6(f)	Whether the Depository Participant has deployed detection and alerting tools. Whether the Depository Participant has created data leakage prevention (DLP) solutions/ processes inclusive of detection, alerting, prevention, containment & response to a data breach/ data leak.
6(g)	Whether the Depository Participant has enforced effective data protection, backup, and recovery measures.
7	**Hardening of Hardware and Software**
7(a)	Whether the Depository Participant only deploys hardened hardware/ software, including replacing default passwords with strong passwords and disabling or removing services identified as unnecessary for the functioning of the system.
7(b)	Whether open ports on networks and systems which are not in use or that can be potentially used for exploitation of data are blocked and measures are taken to secure them.
8	**Application Security in Customer Facing Applications**
8(a)	Whether the Depository Participant's customer facing applications offered over the Internet such as portals containing sensitive or private information and back-office applications, are secured. (Illustrative list of measures for ensuring security in such applications is provided in Annexure C of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018)
9	**Certification of off-the-shelf products**
9(a)	Whether the Depository Participant has ensured that off the shelf products being used for core business functionality (such as Back-office applications) bear Indian Common Criteria Certification of Evaluation Assurance Level 4 provided by Standardization Testing and Quality Certification (STQC), Ministry of Electronics and Information Technology Whether custom developed/ in-house software and components have undergone

Cyber Audit TOR Clause	Checkpoints Description
	intensive regression testing, configuration testing etc. and whether the scope of tests include business logic and security controls as well.
10	**Patch management**
10(a)	Whether the Depository Participant has included all operating systems and applications for updating latest patches on a regular basis. Whether the Depository Participant has established and ensured that patch management procedures include the identification, categorization and prioritization of patches and updates. Whether an implementation timeframe for each category of patches is established, to apply them in a timely manner. Where patches are not available, has the Depository Participant considered virtual patching for protecting systems and networks. Are the patches sourced only from the authorized sites of the OEM.
10(b)	Has the Depository Participant 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 other systems.
11	**Disposal of data, systems, and storage devices**
11(a)	Has the Depository Participant framed suitable policy for disposal of storage media and systems. Whether the critical data/ information on such devices and systems removed by using methods such as crypto shredding/ degauss/ physical destruction as applicable.
11(b)	Has the Depository Participant formulated a data-disposal and data-retention policy to identify the value and lifetime of various parcels of data.
12	**Vulnerability Assessment and Penetration Testing (VAPT)**
12(a)	Has the Depository Participant carried out periodic Vulnerability Assessment and Penetration Tests (VAPT) which inter-alia includes critical assets and infrastructure components like Servers, Networking systems, Security devices, Load balancers, other IT systems pertaining to the activities done as Depository Participant, in order to detect security vulnerabilities in the IT environment and in-depth evaluation of the security posture of the system through simulation of actual attacks on its system and networks.

Cyber Audit TOR Clause	Checkpoints Description
12(b)	Has the Depository Participant conducted VAPT at least once in a financial year. Has the Depository Participant engaged only CERT-In empanelled organizations for conducting VAPT. Whether the final report on said VAPT has been submitted to the Depository after approval from Technology Committee of Depository Participant, within 1 month of completion of VAPT activity.
12(c)	Has the Depository Participant performed vulnerability scanning and conducted penetration testing prior to the commissioning of a new system which is a critical system or part of an existing critical system.
12(d)	In case of vulnerabilities discovered in off-the-shelf products (used for core business) or applications provided by vendors, has the Depository Participant reported them to the vendors and the Depository in a timely manner.
12(e)	Whether any gaps/vulnerabilities detected are remedied on immediate basis and compliance of closure of findings identified during VAPT is submitted to the Depository within 3 months post the submission of final VAPT report.
13	**Monitoring and Detection**
13(a)	Whether the Depository 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. Whether the security logs of systems, applications and network devices exposed to the internet are monitored for anomalies to identify unusual patterns and behaviours.
13(b)	Whether the Depository Participant has implemented suitable mechanisms to monitor capacity utilization of its critical systems and networks that are exposed to the internet to ensure high resilience, high availability, and timely detection of attacks on systems and networks exposed to the internet, for example, controls such as firewalls to monitor bandwidth usage.
13(c)	Whether the Depository Participant is proactively monitoring the cyberspace to identify phishing websites w.r.t. to REs domain and reporting the same to CSIRT¬ Fin/CERT-In for taking appropriate action.

Cyber Audit TOR Clause	Checkpoints Description
14	**Response and Recovery**
14(a)	Whether the alerts generated from monitoring and detection systems are suitably investigated 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.
14(b)	Does the response and recovery plan of the Depository Participant include timely restoration of systems affected by incidents of cyber-attacks or breaches, for instance, offering alternate services or systems to Customers. Whether the Depository Participant has the same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as specified by SEBI for Market Infrastructure Institutions vide SEBI circular CIR/MRD/DMS/17/20 dated June 22, 2012, as amended from time to time
14(c)	Whether the response plan also 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.
14(d)	Whether incidents of loss or destruction of data or systems are thoroughly analysed
14(e)	Whether lessons learned from such incidents are incorporated to strengthen the security mechanism and improve recovery planning and processes.
14(f)	Whether the Depository Participant also conducts suitable periodic drills to test the adequacy and effectiveness of the response and recovery plan. Whether the Depository Participant has conducted Periodic DR drills.
15	**Sharing of Information**
15(a)	Whether all Cyber-attacks, threats, cyber-incidents and breaches experienced by Depository Participant are reported to Depository /CERT-In and SEBI within 6 hours of noticing/ detecting such incidents or having such incidents brought to notice. Whether this information is shared with CERT-In and SEBI through the dedicated e-mail id: incident@cert-in.org.in & sbdp-cyberincidents@sebi.gov.in.
15(b)	The incident shall also be reported to Indian Computer Emergency Response team (CERT-In) in accordance with the guidelines/ directions issued by CERT-In from time to time. Additionally, the Depository Participant, whose systems have been identified as

Cyber Audit TOR Clause	Checkpoints Description
	"Protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC.
15(c)	Whether quarterly reports containing information on cyber-attacks, threats, cyber-incidents and breaches experienced by Depository Participant and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs/ vulnerabilities / threats that may be useful for other Depository Participants, are submitted to Depository within 15 days from the quarter ended June, September, December and March of every year.
16	**Training and Education**
16(a)	Whether the Depository Participant has conducted activities on building Cyber Security and basic system hygiene awareness of staff (with a focus on staff from non-technical disciplines).
16(b)	Whether the Depository Participant conducts periodic training programs to enhance knowledge of IT/ Cyber Security policy and standards among the employees incorporating up-to-date Cyber Security threat alerts and advisories issued by CERT- In/ CSIRT-Fin that may be referred for assistance in conducting exercises for public awareness. Whether the training programs are extended to outsourced staff, vendors etc and whether the training programs are reviewed and updated to ensure that the contents of the program remain current and relevant.
16(c)	Whether the Depository Participant provides training to the employees to avoid clicking on a link in a spear-phishing email, reusing their personal password on a work account, mixing personal with work email and/or work documents, or allowing someone, they should not, use their corporate device, especially in Work from Home environment.
17	**Systems managed by vendors**
17(a)	Where the systems (Back office and other Customer facing applications, IT infrastructure, etc.) of a Depository Participant are managed by vendors and the Depository Participant may not be able to implement some of the aforementioned guidelines directly, whether the Depository Participant has instructed the vendors to adhere to the applicable

Cyber Audit TOR Clause	Checkpoints Description
	guidelines in the Cyber Security and Cyber Resilience policy and obtain the necessary self-certifications from them to ensure compliance with the policy guidelines.
18	**SEBI Compliances**
18(a)	Auditor to ensure implementation of circulars, notices, guidelines, and advisories published by CERT-In/ CSIRT-Fin and SEBI and mention: a. Adherence to all such circulars, notices, guidelines, and advisories published b. Reporting adherences based on prescribed periodicity in point (a) above
19	**Advisory for Financial Sector Organizations:**
19(a)	Whether the Depository Participant has complied with the SEBI circular no. SEBI/HO/MIRSD2/DOR/CIR/P/ 2020/221 dated November 03, 2020, for Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions.
20	**Cyber Security Advisory - Standard Operating Procedure (SOP)**
20(a)	Whether all aspects of the Cyber Security Advisory - Standard Operating Procedure (SOP) issued by SEBI have been complied by the Depository Participant
20(b)	Whether the Depository Participant has a well-documented Cyber Security incident handling process document (Standard Operating Procedure - SOP) in place. Whether such policy is approved by Board of the Depository Participant (in case of corporate Depository Participant), Partners (in case of partnership firms) or Proprietor (in case of sole proprietorship firm) as the case may be and is reviewed annually by the "Designated Officer" and "Technology Committee" as constituted under SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018, for review of Security and Cyber Resilience policy.
20(c)	Has the Depository Participant examined the Cyber Security incident and classified the Cyber Security incidents into High/ Medium/ Low as per their Cyber Security incident handling process document. Has the Cyber Security incident handling process document defined decision on Action/ Response for the Cyber Security incident based on severity.
20(d)	Has the Depository Participant reported the Cyber Security incident to Indian Computer Emergency Response Team (CERT-In).

Cyber Audit TOR Clause	Checkpoints Description
20(e)	Whether the Depository Participant has provided the reference details of the reported Cyber Security incident with CERT-In to the Depository and SEBI. Whether the Depository Participant has provided details, regarding whether CERT-In team is in touch with the Depository Participant for any assistance on the reported Cyber Security incident. If the Cyber Security incident is not reported to CERT-In, has the Depository Participant submitted the reasons for the same to the Depository and SEBI. Whether the Depository Participant has communicated with CERT-In/ Ministry of Home Affairs (MHA)/ Cyber Security Cell of Police for further assistance on the reported Cyber Security incident.
20(f)	Whether the Depository Participant has submitted details about whether the Cyber Security incident has been registered as a complaint with law enforcement agencies such as Police or its Cyber Security cell. If yes, are the details provided to Depository and SEBI. If no, then the reason for not registering complaint has been provided to Depository and SEBI.
20(g)	Whether the details of the reported Cyber Security incident submitted to various agencies by the Depository Participant are also submitted to Division Chiefs (in-charge of divisions at the time of submission) of DOS-MIRSD and CISO of SEBI in accordance with SEBI email dated April 16, 2021 on Standard Operating Procedure (SOP) for handling cyber security incidents
20(h)	The Designated Officer of the Depository Participant (appointed in terms of para 6 of the SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018) shall continue to report any unusual activities and events within 6 hours of receipt of such information as well as submit the quarterly report on the cyber-attacks & threats within 15 days after the end of the respective quarter in the manner as specified in Depository Participant circular.
20(i)	Has the Depository Participant complied with Advisory for SEBI Regulated Entities (REs) regarding Cybersecurity best practices - SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/032 dated February 22, 2023
21	**Security of Cloud Services**

Cyber Audit TOR Clause	Checkpoints Description
21(a)	Whether the Depository Participant checks public accessibility of all cloud instances in use. Whether the Depository Participant ensures that no server/bucket is inadvertently leaking data due to inappropriate configurations.
21(b)	Whether the Depository Participant ensures proper security of cloud access tokens and ensures that the tokens are not exposed publicly in website source code, any configuration files etc.
21(c)	Whether the Depository Participant has implemented appropriate security measures for testing, staging and backup environments hosted on cloud. Does the Depository Participant ensures that the production environment is kept properly segregated from these. Whether the Depository Participant disables/removes older or testing environments if their usage is no longer required.
21(d)	Whether the Depository Participant has considered employing hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments.
21(e)	Whether the Depository Participant has complied with the SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 dated March 06, 2023 for cloud framework