



Central Depository Services (India) Limited

Convenient ⊕ Dependable ⊕ Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

CDSL/RISK/DP/POLCY/2024/301

June 06, 2024

SUBMISSION OF ANNUAL SYSTEM AUDIT REPORT

Depository Participants are advised to refer to CDSL **Communiqué CDSL/A,I&C/DP/POLCY/2023/298 dated May 16, 2023**, on 'Submission of Annual System Audit 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 report has been modified (enclosed as Annexure I). 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 advised to refer to the user manual for submitting the report enclosed as Annexure II and III (The auditor appointed by the DP shall refer to Annexure II for instructions on submitting the information and the designated officer of the DP shall refer to Annexure III for instructions on submitting the report). DPs are required to ensure compliance by submitting the system audit report as per the schedule given below:

Additionally, Participants (DPs) 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' This is a mandatory requirement.



Central Depository Services (India) Limited

Convenient ⊕ Dependable ⊕ Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

Report	Periodicity/ Frequency	Due date of submission	Action Taken Report (ATR) Submission (if applicable)
Annual System Audit Report (Cyber Security Annual Report)	Annually (Online submission on https://auditweb.cdslindia.com . For user manual, refer Annexure II and III)	Within three months of the end of the financial year. i.e. by 30th June.	Within three months from the date of submission. i.e. 30 th September.

Queries regarding this communiqué may be sent to CDSL – Helpdesk through e-mail on dpntasupport@cdslindia.com or dpinfosec@cdslindia.com or call us on 022-62343333.

**For and on behalf of
Central Depository Services (India) Limited**

sd/-

**Ashwin Lalchandani
Assistant Vice President – Risk Management**



Central Depository Services (India) Limited

Convenient ⊕ Dependable ⊕ Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

Annexure I

Audit TOR Clause	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, are provided in the policy document? Is the policy document approved by the Board / Partners / Proprietor of the organization? Is the policy reviewed periodically or at least on annual basis?
1(b)	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.
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 their subsequent revisions, if any, from time to time?



Central Depository Services (India) Limited

Convenient ⊕ Dependable ⊕ Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

Audit TOR Clause	Description
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 of processes 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 and events 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 and technology committee periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen Cyber Security and cyber 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



Central Depository Services (India) Limited

Convenient ⊕ Dependable ⊕ Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

Audit TOR Clause	Description
2(d)	Whether Participant has identified 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
I	Access Control
3(a)	Any access to Participants' systems, applications, networks, databases, etc., should be for a defined purpose and for 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 to supervise 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 other computer resources, have been subjected to stringent supervision, monitoring and access restrictions?



Central Depository Services (India) Limited

Convenient ⊕ Dependable ⊕ Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

Audit TOR Clause	Description
3(g)	Whether 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 Participant's critical IT infrastructure?
3(h)	Whether User Management addresses deactivation of access of privileges of users 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/visitors are properly supervised by ensuring at the minimum that outsourced staff/visitors are 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 equipment room, 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)



Central Depository Services (India) Limited

Convenient ⊕ Dependable ⊕ Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

Audit TOR Clause	Description
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 offered over 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 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)
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 4 which is being provided by Standardisation Testing and Quality Certification (STQC) (Ministry of Electronics and Information Technology)(except Custom developed / in-house software and components need not obtain the certification,



Central Depository Services (India) Limited

Convenient ⊕ Dependable ⊕ Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

Audit TOR Clause	Description
	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 other systems?
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 Penetration Testing (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 empanelled 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.



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

Audit TOR Clause	Description
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 to monitor capacity utilization of its critical systems 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) as specified 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?



Central Depository Services (India) Limited

Convenient ⊕ Dependable ⊕ Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

Audit TOR Clause	Description
5(d)	Whether any incident of loss or destruction of data or systems have been thoroughly analysed 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 the aforementioned response and recovery plan?
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 on building 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 enhance knowledge 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 ensure that 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, whether 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?



Central Depository Services (India) Limited

Convenient ⊕ Dependable ⊕ Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

Audit TOR Clause	Description
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
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?



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

Annexure II

FOR AUDITOR

Step 1- Log in Into Audit application by using the below link:-

<https://auditweb.cdslindia.com/Login.aspx>

- Now Sign in using 'Login Type-CISA_Auditor'.
- Now enter User ID & Password and click on "Sign In" button.

Step 2- Select "Cyber Security Annual Report" in the 'Select Audit Type' tab as highlighted below.



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

Central Depository Services (India) Limited
Convenient • Dependable • Secure

AUDIT APPLICATION

Reports

Select Audit Type: --Select--

Select Audit Month: --Select--

Select DP / RTA: --Select--

Options for Select Audit Type:

- CYBER MULTIPLE INCIDENT REPORT
- CYBER ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING REPORT
- CYBER INCIDENT REPORT
- CYBER SECURITY ANNUAL REPORT**
- IMPLEMENTATION OF CYBER SECURITY AND CYBER RESILIENCE FRAMEWORK
- VAPT REPORT
- SYSTEM AUDIT REPORT

Step 3- Select the Year for which the report is to be submitted,

a. Select “March 2024” in “Audit Month”

Central Depository Services (India) Limited
Convenient • Dependable • Secure

AUDIT APPLICATION

Reports

Select Audit Type: CYBER SECURITY ANNUAL REPORT

Select Audit Month: --Select--

Select DP / RTA: --Select--

Options for Select Audit Month:

- Select--
- March-2021
- March-2022
- March-2023
- March-2024

Step 4- Select the DP ID and DP Name in the ‘**Select DP / RTA**’ tab and click on ‘**Confirm**’

Step 5- The below screen will be presented once the user is logged in:



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

The screenshot displays the 'AUDIT APPLICATION' interface for 'CYBER SECURITY ANNUAL REPORT'. The form includes fields for 'Audit Type', 'Period', 'Schedule No', 'DP Name(ID)', and 'DP ID'. Below these fields, there is a section for 'Number of Findings/Observation' with three columns: 'High', 'Medium', and 'Low', each containing a text input field. The 'High' field is highlighted with a purple background. Below the form, there is a table with the following columns: 'Auditor Clause', 'Checkpoint Description', 'Compliance Status', 'Management Comments', 'Description of Findings/ Observations/Reason why the TOR Clause is not applicable to the DP', 'Target Closure Date (dd/mm/yyyy)', and 'Severity Finding'. The table is currently empty. The footer of the page contains the text: 'Copyright © 2019 - Audit Team, Central Depository Services (India) Ltd. All rights reserved.'

Step 6- The auditor shall mention the number of findings/ observation for each of risk.

This screenshot is identical to the one above, but with a black arrow pointing to the 'High' input field in the 'Number of Findings/Observation' section, indicating where the auditor should enter the number of findings for high risk.



Central Depository Services (India) Limited

Convenient ⊕ Dependable ⊕ Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

Step 7- The auditor has been given access to fill the below mentioned fields.

- a. **Compliance Status** – The Auditor shall mention whether the DP is complying with the said checkpoint or not. The options which Auditor can select are **Complied, Not Complied and NA(in case the checkpoint is not applicable to the DP)**.
- b. **Description of Findings/ Observations/Reason why the TOR Clause is not applicable to the DP** – The Auditor shall mention his **observations** in case the DP has not complied with the Checkpoint/ the reason why the said checkpoint is **Not Applicable** to the DP. In case the DP is complying with the said checkpoint, then the auditor shall mention 'Not Applicable' in the said section.
- c. **Severity Finding** – The Auditor shall mention the Severity of the observation i.e. High, Medium or Low

Step 8- Once the form is filled, the auditor shall click on '**Save**'

If any **error** is faced while uploading the report/declaration/submitted the form, request you to send an email to the below email addresses **along with the screenshot of the error**.

1. dpinfosec@cdslindia.com
2. helpdesk@cdslindia.com



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

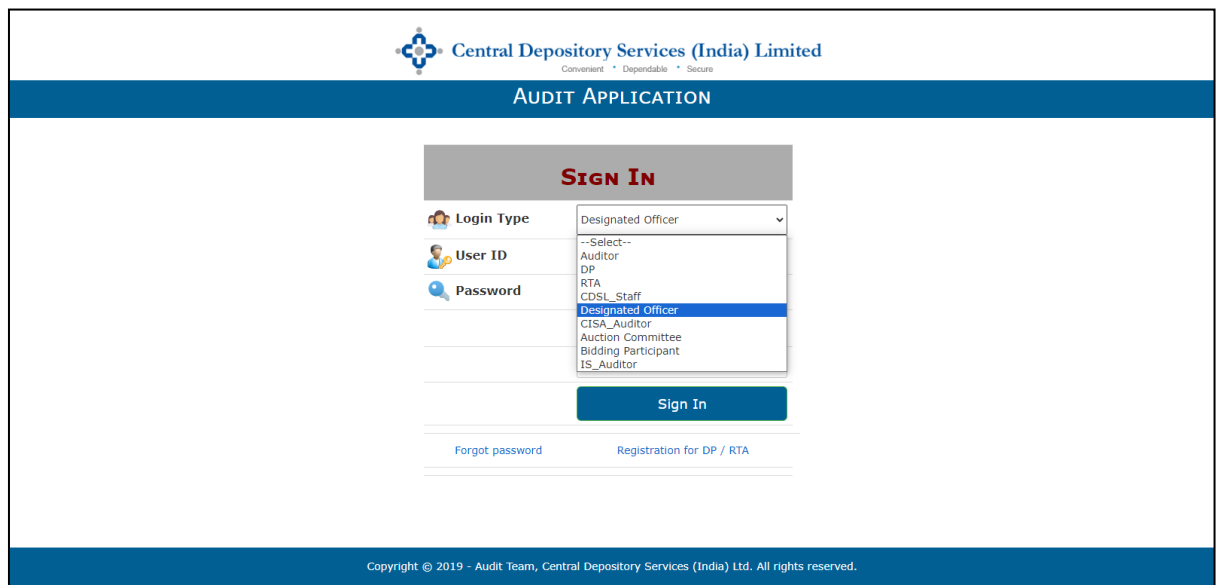
Annexure III

FOR DESIGNATED OFFICER

Step 1- Log in Into Audit application by using the below link:-

<https://auditweb.cdslindia.com/Login.aspx>

- Now Sign in using 'Login Type-Designated officer'.
- Now enter User ID & Password and click on "Sign In" button.



Central Depository Services (India) Limited
Convenient + Dependable + Secure

AUDIT APPLICATION

SIGN IN

Login Type	Designated Officer
User ID	--Select--
Password	Auditor
	DP
	RTA
	CDSL_Staff
	Designated Officer
	CISA_Auditor
	Auction Committee
	Bidding Participant
	IS_Auditor

Sign In

[Forgot password](#) [Registration for DP / RTA](#)

Copyright © 2019 - Audit Team, Central Depository Services (India) Ltd. All rights reserved.



Central Depository Services (India) Limited

Convenient \oplus Dependable \oplus Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

Step 2- Select “Cyber Security Annual Report” in the ‘Select Audit Type’ tab as highlighted below.

The screenshot shows the 'AUDIT APPLICATION' form. The 'Select Audit Type' dropdown menu is open, displaying a list of report types. The 'CYBER SECURITY ANNUAL REPORT' option is highlighted in purple, and a black arrow points to it from the right. Other options in the list include 'CYBER MULTIPLE INCIDENT REPORT', 'CYBER ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING REPORT', 'CYBER INCIDENT REPORT', 'IMPLEMENTATION OF CYBER SECURITY AND CYBER RESILIENCE FRAMEWORK', 'VAPT REPORT', and 'SYSTEM AUDIT REPORT'. Below the dropdown, there are links for 'View Cyber Report', 'VAPT Compliance', 'VAPT Resubmission', 'Cyber Audit Compliance Report', and 'Cyber RCA Report'. At the bottom, there are links for 'System Audit Compliance Report', 'Go to Login', and 'Change Password'. A green bar at the bottom left contains the text 'FAQ'. The footer text reads 'Copyright © 2019 - Audit Team, Central Depository Services (India) Ltd. All rights reserved.'

Step 3- Select the Year for which the report is to be submitted,

- a. Select "March 2024" in “Audit Month”

The screenshot shows the 'AUDIT APPLICATION' form. The 'Select Audit Type' dropdown menu is now closed and shows 'CYBER SECURITY ANNUAL REPORT'. The 'Select Audit Month' dropdown menu is open, displaying a list of months. The 'March-2024' option is highlighted in dark blue, indicating it is the selected option. Other options in the list include 'March-2021', 'March-2022', and 'March-2023'. The rest of the form, including the 'Select DP / RTA' field and the bottom navigation links, remains the same as in the previous screenshot. The footer text reads 'Copyright © 2019 - Audit Team, Central Depository Services (India) Ltd. All rights reserved.'

Step 4- Select the DP ID and DP Name in the ‘Select DP / RTA’ tab and click on ‘Confirm’



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

Step 5- The below screen will be presented once the user is logged in:

Step 6- The 'Designated Officer' is given access to fill only the below mentioned fields:

- Management Comments
- Target Closure Date (dd/mm/yyyy)

Hence, once the CISA Auditor has provided his observations, the Designated Officer of the DP Shall login and fill the abovementioned columns. Illustrative Scenarios have been described below for clarity.

- Scenario 1:** If the auditor has provided 'Not Complied' Compliance Status for any of the checkpoints, then the DP shall mention, the reason why it has not complied in the 'Management Comments' section and provide the Target Closure date for rectifying/complying with the observation in the **Target Closure Date (dd/mm/yyyy)** section.
- Scenario 2:** If the auditor has provided 'NA' Compliance Status for any of the checkpoints, then the DP shall mention, the reason why it is **Not Applicable** in the 'Management Comments' section and mention **30/09/2024** in the **Target Closure Date (dd/mm/yyyy)** section.
- Scenario 3:** If the auditor has provided 'Complied' Compliance Status for any of the checkpoints, then the DP shall mention, 'Not Applicable' in the 'Management Comments' section and mention **30/09/2024** in the **Target Closure Date (dd/mm/yyyy)** section.



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

Step 7- The DP shall follow Step 6 for all the Checkpoints.

Step 8- Under 'Attach File - Declaration from the MD/ CEO/ Partners/ Proprietor Certifying Compliance' under the 'Audit Findings and Compliance Declaration' section, the DP shall upload the declaration as required under SEBI Circular **SEBI/HO/MIRSD/TPD/P/CIR/2022/80** dated **June 07, 2022**, from the MD/ CEO/ Partners/ Proprietors of the DP certifying compliance with **all SEBI Circulars and advisories related to Cyber security issued from time to time (Screenshot below)**.

10. ADDITIONAL INFORMATION ABOUT PARTICIPANT

11. DATA LEAKAGE

AUDIT FINDINGS AND COMPLIANCE DECLARATION

Sr. No	Type of Findings	Count
1	Non-conformity (Major)	<input type="text"/>
2	Non-conformity (Minor)	<input type="text"/>
3	Observations	<input type="text"/>
4	Opportunity for improvement	<input type="text"/>

Attach File - Declaration from the MD/ CEO/ Partners/ Proprietor Certifying Compliance

Choose File

Attach File

Choose File

Copyright © 2019 - Audit Team, Central Depository Services (India) Ltd. All rights reserved.

Step 9- Under 'Attach File' section at the end of the page the DP shall upload the physical copy of the report wherein the checkpoints mentioned in the Communique are clearly stated and the Auditor's observations and Management Comments and the Target Closure date are clearly mentioned.

Furthermore, the Audit report shall be on the letterhead of the Auditor and shall also be signed and stamped. It shall also contain the membership number of the auditor from the relevant authority and the expiration date of the membership number.



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

The screenshot shows a web interface with a list of menu items on the left side, including: 4. MONITORING AND DETECTION, 5. RESPONSE AND RECOVERY, 6. SHARING OF INFORMATION, 7. TRAINING AND EDUCATION, 8. SYSTEMS MANAGED BY VENDORS, 9. AI/ML, 10. ADDITIONAL INFORMATION ABOUT PARTICIPANT, 11. DATA LEAKAGE, and AUDIT FINDINGS AND COMPLIANCE DECLARATION. Below the list is an 'Attach File' section with a 'Choose File' button, a file name field containing 'file chosen', an 'Upload' button, and a file size indicator '38'. At the bottom of the form are 'Save' and 'Submit to CDSL' buttons. A copyright notice at the bottom reads: 'Copyright © 2019 - Audit Team, Central Depository Services (India) Ltd. All rights reserved.'

Step 10- Once the form is filled and the declaration and the report is uploaded, the DP shall click on ‘**Submit to CDSL**’

If any **error** is faced while uploading the report/declaration/submitting the form, request you to send an email to the below email addresses **along with the screenshot of the error**.

1. dpinfosec@cdslindia.com
2. helpdesk@cdslindia.com