



# Central Depository Services (India) Limited

Convenient + Dependable + Secure

## COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

CDSL/IS/DP/POLCY/2025/622

September 15, 2025

### SUBMISSION OF COMPLIANCE FOR CLOSURE OF OBSERVATIONS RAISED DURING CYBER AUDIT

Depository Participants (DPs) are advised to refer to Communique **CDSL/RISK/DP/POLCY/2024/534** September 16, 2024 and **CDSL/IS/DP/POLCY/2025/381** June 09, 2025, on 'Submission of Cyber Audit Report'.

Any observation raised by the auditor during the audit shall be remedied on an immediate basis and should be certified by the auditor. The compliance of closure of findings identified shall be submitted to CDSL **within 3 months** from the due date of submission of report.

DPs are advised to submit compliance of closure of observations raised during the audit for the financial year 2024-2025 **on or before September 30, 2025**. The User Manual for submission of the same is enclosed as **Annexure A**. DPs are requested to take note of the above and ensure compliance.

Queries regarding this communiqué may be addressed to CDSL –emails may be sent to: [dpinfosec@cdslindia.com](mailto:dpinfosec@cdslindia.com) and connect through our IVR Number 022-62343333.

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

sd/-

**Mrugen Vijay Munjpara  
Assistant Vice President – Information Security**

Internal



# Central Depository Services (India) Limited

Convenient + Dependable + Secure

## COMMUNIQUE TO DEPOSITORY PARTICIPANTS

### Annexure A

#### Guidelines to submit Cyber Audit ATR (Action Taken Report)

##### CISA AUDITOR SCREEN

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.

The screenshot shows the login interface for the CISA Auditor. The page has a blue header with the Central Depository Services (India) Limited logo and the text 'AUDIT APPLICATION'. Below the header, there is a 'SIGN IN' section. It includes a 'Login Type' dropdown menu currently set to 'CISA\_Auditor'. Below this are fields for 'User ID' and 'Password'. The password field has a strength indicator showing '304791' and a 'Sign In' button. At the bottom of the login section, there are links for 'Forgot password' and 'Registration for DP / RPA'. The footer contains copyright information: 'Copyright © 2019 - Audit Team, Central Depository Services (India) Ltd. All rights reserved.'

2. **Enter the OTP:** You will receive the OTP on both your CISA registered mobile number and email Id.

The screenshot shows the OTP verification interface for the CISA Auditor. The page has a blue header with the Central Depository Services (India) Limited logo and the text 'AUDIT APPLICATION'. Below the header, there is a 'LOGIN OTP' section. It includes an 'Enter OTP' field with the value '715675'. Below this field, there is an 'OTP Time' of '00:09:38' and a 'Verify OTP' button. A warning message 'Do not refresh the page' is displayed. The footer contains copyright information: 'Copyright © 2019 - Audit Team, Central Depository Services (India) Ltd. All rights reserved.'



# Central Depository Services (India) Limited

Convenient + Dependable + Secure

## COMMUNIQUE TO DEPOSITORY PARTICIPANTS

3. Then select audit type “Cyber Security Audit ATR” from the Drop down.

Select Audit month, the DP ID and DP Name in the ‘**Select DP / RTA**’ tab and click on ‘**Confirm**’.

**AUDIT APPLICATION**

Select Audit Type	CYBER SECURITY AUDIT ATR	▼
Select Audit Month		▼
Select DP / RTA		▼

Confirm

4. The below screen will be presented once the user is logged in. Enter all the details mentioned below. **All the details below will be auto populated.**

**AUDIT APPLICATION**

CYBER SECURITY AUDIT ATR (Action Taken Report)

* Date	8/25/2025 4:21:26 PM	* DP Name	
* DP ID		* Period	

\* Name of CERT-In empanelled entity :

XXXX

\* CERT-In empanelment validity expiry Date (DD- MM- YYYY):

29-09-2025

Last date of Submission 30-Sep-2025 . If the report is submitted after this date, then it will be treated as non compliance.

5. Kindly note that only the non-compliant points will be displayed here

The ‘**CISA Auditor**’ is given access to fill only the below mentioned fields:

- Compliance Status.
- Description of Findings/Reason why the TOR clause is not applicable to DP.
- Severity Level.

**4. PHYSICAL SECURITY**

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)	Severity Level
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.	COMPLIED ▼			dd-mm-yyyy	Select ▼
4 (b)	Whether physical access to the critical systems is revoked immediately if the same is no longer required.	COMPLIED ▼			dd-mm-yyyy	Select ▼

Save

Save & Submit To DP Cancel



# Central Depository Services (India) Limited

Convenient ⊕ Dependable ⊕ Secure

## COMMUNIQUE TO DEPOSITORY PARTICIPANTS

---

Once all details have been entered, kindly click on the 'SAVE' button in every segment

6. Once all segments have been saved, proceed by clicking on the '**SAVE & Submit to DP**' button. The report status will reflect as **Report submitted to DP**.

The screenshot shows a web interface with a 'Save' button at the top left. Below it is a red status bar with the text 'Report Status - Report Submitted To DP'. At the bottom left, there are two buttons: 'Save & Submit to DP' (blue) and 'Cancel' (red).



# Central Depository Services (India) Limited

Convenient + Dependable + Secure

## COMMUNIQUE TO DEPOSITORY PARTICIPANTS

### DESIGNATED OFFICER LOGIN

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.

The screenshot shows the 'SIGN IN' page of the Central Depository Services (India) Limited Audit Application. The page has a blue header with the company logo and name. Below the header, there is a 'SIGN IN' section with a dropdown menu for 'Login Type' set to 'Designated Officer'. There are input fields for 'User ID' and 'Password'. A 'Sign In' button is located below the password field. There are also links for 'Forgot password' and 'Registration for DP / RTA'. The footer contains copyright information: 'Copyright © 2019 - Audit Team, Central Depository Services (India) Ltd. All rights reserved.'

2. **Enter the OTP:** You will receive the OTP on both your DP's registered mobile number and email Id.

The screenshot shows the 'LOGIN OTP' page of the Central Depository Services (India) Limited Audit Application. The page has a blue header with the company logo and name. Below the header, there is a 'LOGIN OTP' section with an 'Enter OTP' field and a 'Verify OTP' button. There is a timer for the OTP validity: 'OTP Time :- 00:09:56'. There is also a note: 'Do not refresh the page'. The footer contains copyright information: 'Copyright © 2019 - Audit Team, Central Depository Services (India) Ltd. All rights reserved.'



# Central Depository Services (India) Limited

Convenient + Dependable + Secure

## COMMUNIQUE TO DEPOSITORY PARTICIPANTS

- Then select audit type “Cyber Security Audit ATR” from the Drop down.  
Select the DP ID and DP Name in the ‘**Select DP / RTA**’ tab and click on ‘**Confirm**’.

**AUDIT APPLICATION**

Select Audit Type	CYBER SECURITY AUDIT ATR	▼
Select Audit Month		▼
Select DP / RTA		▼

Confirm

- The below screen will be displayed once the user is logged in. **All the details below will be auto-populated**

**AUDIT APPLICATION**

CYBER SECURITY AUDIT ATR (Action Taken Report)

* Date	8/25/2025 5:12:48 PM	* DP Name	
* DP ID		* Period	
* Name of CERT in empanelled entity :		XXXX	
* CERT in empanelment validity expiry Date (DD- MM- YYYY):		29-05-2025	

Last date of Submission 30-Sep-2025 . If the report is submitted after this date, then it will be treated as non compliance.

- The ‘**Designated Officer**’ is given access to fill only the below mentioned fields:
  - Management Comments
  - Target Closure Date (dd/mm/yyyy)

**1. GOVERNANCE**

**2. IDENTIFICATION**

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)	Severity Level
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.	NOT COMPLIED ▼	XXXX	XXXX	27-08-2025	High ▼
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.	NA ▼	XXXX	XXXX	dd-mm-yyyy	Select ▼

Save



# Central Depository Services (India) Limited

Convenient + Dependable + Secure

## COMMUNIQUE TO DEPOSITORY PARTICIPANTS

6. Save all segments, then click **SAVE** and generate the PDF to review the details before uploading.

DP ID		DP name		Report type		Period	
				Cyber Security Audit ATR			
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	Severity Finding	
1 (a)	Has the Depository Participant formulated a comprehensive Cyber Security and Cyber Resilience	not complied	test	test	27-08-2025	critical	

Please make sure the file name remains unchanged after downloading, printing, and signing i.e., **dp\_id\_Cyber\_Sec\_ATR\_date**.

- For example: **30000\_Cyber\_Sec\_ATR\_20250903 (yyyymmdd)**

7. Report status will show *File Generated*. Please upload the file and then click on **Submit to CDSL**

Attach File -Attach only Cyber Security Audit ATR

Choose File

No file chosen

Upload

38100\_Cyber\_Sec\_ATR\_25-08-2025\_05\_32\_26.pdf

☐ Declaration : I hereby declare that the information given above and in the enclosed documents is true to the best of my knowledge.

Report Status -- The file has been generated. Please upload then click on 'Submit to CDSL'.

Save

Generate PDF

Submit to CDSL

Cancel

Before submission, please click on declaration check box

8. After submission to CDSL, the report status will reflect as **Submitted**

Attach File -Attach only Cyber Security Audit ATR

Choose File

No file chosen

Upload

38100\_Cyber\_Sec\_ATR\_25-08-2025\_05\_32\_26.pdf

☒ Declaration : I hereby declare that the information given above and in the enclosed documents is true to the best of my knowledge.

Report Status -- Submitted

Save

Generate PDF

Submit to CDSL

Cancel



# Central Depository Services (India) Limited

Convenient ⊕ Dependable ⊕ Secure

## COMMUNIQUE TO DEPOSITORY PARTICIPANTS

---

### DPs are advised to take note of the following:

- CISA Auditor registration/mapping is carried out through the DP login, and the same auditor can then proceed with the submission.
- Each submission is permitted for a single auditor only.
- If you want to change your auditor, ensure the previous auditor is deleted before adding or mapping a new one through DP login.
- If the compliance status for any clause in the checkpoint description is marked as **"Complied"** the fields for Description of Findings, Target Date, and Severity will be disabled.
- If the compliance status for any clause in the checkpoint description is marked as **"Not Complied"** then Management Comments, Description of Findings, Target Date, and Severity fields are mandatory.
- If the compliance status for any clause is marked as **"Not Applicable"** the Management Comments and Description of Findings fields are mandatory.
- The audit report must be on the letterhead containing the name of the auditor, audit firm, Cert-In empanelment expiry date and valid signature
- The audit report must include the DP Name and DP ID.
- Audit period must be clearly mentioned.
- Compliance status must be clearly stated as Complied / Not Complied / Not Applicable.
- Kindly ensure each subpoints of the Checkpoint Description are duly filled in and **SAVED** before submitting it to CDSL. If the details are not saved prior to submission, the data may not be recorded in the system which may result in incomplete or missing information at the time of submission.

If any error is faced while submitting the report, request you to send an email on [dpinfosec@cdslindia.com](mailto:dpinfosec@cdslindia.com) along with the screenshot of the error.

\*\*\*\*