



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

CDSL/IS/DP/POLCY/2025/623

September 15, 2025

SUBMISSION OF COMPLIANCE FOR CLOSURE OF OBSERVATIONS RAISED DURING ANNUAL SYSTEM AUDIT

Depository Participants (DPs) are advised to refer to Communique **CDSL/RISK/DP/POLCY/2024/536** September 16, 2024 and **CDSL/IS/DP/POLCY/2025/380** June 09, 2025, on 'Submission of Annual System 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 audit period April 2024- March 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 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



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUE TO DEPOSITORY PARTICIPANTS

Annexure A

Guidelines to submit System 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.

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



Central Depository Services (India) Limited

Convenient ⊕ Dependable ⊕ Secure

COMMUNIQUE TO DEPOSITORY PARTICIPANTS

3. Then select audit type “System 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	SYSTEM AUDIT ATR
Select Audit Month	
Select DP / RTA	
<button>Confirm</button>	

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

AUDIT APPLICATION	
SYSTEM AUDIT ATR (Action Taken Report)	
* Date	8/25/2025 7:17:33 PM
* DP ID	
* DP Name	
* Period	
* Name of the Auditor :	test
* Auditor Firm Expiry Date (DD-MM-YYYY):	27-08-2025
Last date of Submission 28-Feb-2026 . If the report is submitted after this date, then it will be treated as non compliance.	

5. Please note that only the points marked as non-compliant will be displayed.

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.



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

22. INFORMATION RISK MANAGEMENT

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
22 (a)	"Has the organization implemented a comprehensive risk assessment, governance, and management framework. Has the organization developed detailed risk management program that incorporates standards, guidelines, templates, processes, risk catalogues, checklist, measurement metrics and calendar to support and evidence risk management activities. If yes, is the risk management program calendar reviewed periodically. Are the risk identification and assessment processes repeated periodically to review existing risks and identify new risks. Are risks reported to the Senior Management through reports and dashboards on a periodic basis. Are evidences available to demonstrate risk decisions such as Risk Mitigation, Risk Acceptance, Risk Transfer, Risk Avoidance by Senior Management. Is there a dedicated Risk Management Team for managing Risk and Compliance activities Is the Risk Management Framework automated. Are SLAs defined for all risk management activities. Has the organization defined procedure/process for Risk Acceptance. Are reports and real time dashboards published in order to report/track risks"	NOT COMPLIED ▼		aaa	dd-mm-yyyy	Critical ▼
22 (b)	"Has the organization deployed alert mechanism for detecting malfunctioning of device, software, and backup system"	NA ▼		aaa	dd-mm-yyyy	-Select- ▼

Save

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

- 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**.

Save

Report Status - Report Submitted To DP.

Save & Submit to DP

Cancel



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.

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



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUE TO DEPOSITORY PARTICIPANTS

3. Then select audit type “System 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	SYSTEM AUDIT ATR	▼
Select Audit Month		▼
Select DP / RTA		▼

Confirm

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

AUDIT APPLICATION

SYSTEM AUDIT ATR (Action Taken Report)

* Date	8/25/2025 7:43:47 PM	* DP Name	
* DP ID		* Period	
*Name of the Auditor :	test		
*Auditor Firm Expiry Date (DD-MM-YYYY):	02-07-2025		

Last date of Submission 28-Feb-2026 . If the report is submitted after this date, then it will be treated as non compliance.

5. The ‘**Designated Officer**’ is given access to fill only the below mentioned fields:

- Management Comments
- Target Closure Date (dd/mm/yyyy), in case of any open finding

2. PASSWORD 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
2 (a)	"Organization Access Policy Whether the organization has a well-documented policy that provides for a password policy as well as access control policy for the depository applications / Depository Participants systems."	COMPLIED			dd-mm-yyyy	-Select-
2 (b)	"Authentication Capability Whether the system authenticates user credentials by means of a password before allowing the user to login, and whether there is a system for authentication such as two-factor authentication."	NA	SSS	SSS	dd-mm-yyyy	-Select-
2 (c)	"Password Best Practices Whether there is a system provision for masking of password, system prompt to change default password on first login, disablement of user id on entering multiple wrong passwords (as defined in the password policy document), periodic password change mandate and appropriate prompt to user, strong parameters for password, deactivation of dormant user id, etc."	NOT COMPLIED	SSS	SSS	28-08-2025	Critical
2 (d)	"The password policy/standard should be documented. The installed systems password features should include: a) The installed system uses passwords for authentication. b) The system requests for identification and new password before login into the system. c) The password is masked at the time of entry. System authenticates user with a username and password as first level of security. System mandates changing of password when the user logs in for the first time. Automatic disablement of the user on entering erroneous password in excess of the number of attempts allowed as per the password policy/system feature. The system provides for automatic expiry of passwords at the end of a reasonable duration (maximum 90 Days) and re-initialisation of access on entering fresh passwords. Prior intimation is given to the user before such expiry. System controls to ensure that the password is alphanumeric (preferably with one special character), instead of just being alphabets or just numerical. System controls to ensure that the changed password cannot be the same as any of the passwords used previously as per the password policy/system feature. System controls to ensure that the login id of the user and password should not be the same. System controls to ensure that the password should be of minimum eight characters. User/Client is deactivated if the same is not used for a continuous period of 12 (Twelve) months from date of last use of the account. System allows user to change their passwords at their discretion and frequency."	COMPLIED			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	
				System 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	
2 (a)	"Organizational Access	complied					

Please make sure the file name remains unchanged after downloading, printing, and signing i.e., **dp_id_System_Audit_ATR_date**.

- For example: **30000_System_Audit_ATR_20250903 (yyyymmdd)**

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

[22. INFORMATION RISK MANAGEMENT](#)

Attach File

Choose File No file chosen

Upload 38100_System_Audit_ATR_25-08-2025_07_47_17.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 and 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

Choose File No file chosen

Upload 38100_System_Audit_ATR_25-08-2025_07_47_17.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, Audit firm 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 along with the screenshot of the error.
