



# Central Depository Services (India) Limited

Convenient + Dependable + Secure

## COMMUNIQUE TO DEPOSITORY PARTICIPANTS

CDSL/IS/DP/POLCY/2025/380

June 09, 2025

### SUBMISSION OF SYSTEM AUDIT REPORT

Depository Participants (DPs) are advised to refer Circular No. **CDSL/RISK/DP/POLCY/2024/536** **September 16, 2024**, for submitting the System Audit Report.

In view of the above, Depository Participants are hereby informed that CDSL has developed a facility for online submission for System Audit Report through audit web portal. The deadline for **System Audit** report submission is on or before **30<sup>th</sup> June 2025**.

Please follow the submission guidelines as provided in **Annexure A** for submitting the **System Audit** report to CDSL.

DPs shall also submit a declaration from its MD/ CEO/ Partners/ Proprietors certifying compliance by DPs with all the circulars and advisories related to System Audit from time to time, along with the System Audit report.

Queries regarding this communiqué may be sent to CDSL – on [dpinfosec@cdslindia.com](mailto:dpinfosec@cdslindia.com) or call us on 022-62343333.

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

sd/-

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

Public



# Central Depository Services (India) Limited

Convenient + Dependable + Secure

## COMMUNIQUE TO DEPOSITORY PARTICIPANTS

Annexure A

### Guidelines to submit System Audit 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 DP's registered mobile number and email Id.



# Central Depository Services (India) Limited

Convenient + Dependable + Secure

## COMMUNIQUE TO DEPOSITORY PARTICIPANTS

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

- The below screen will be presented once the user is logged in. Enter all the details mentioned below.

**Fields marked with an asterisk (\*) are mandatory.**



# Central Depository Services (India) Limited

Convenient ⊕ Dependable ⊕ Secure

## COMMUNIQUE TO DEPOSITORY PARTICIPANTS

---

5. Please ensure that all necessary details specified in the Terms of Reference (TOR) for the System Audit Report, as outlined in Circular No: **CDSL/RISK/DP/POLCY/2024/536 dated September 16, 2024**, are duly entered.

### Checkpoints Description:

1. Software Change Management – The system auditor should check whether proper procedures have been followed, and proper documentation has been maintained for the following:
2. Password Security
3. Session Management (Mobile Application / Client Server Application / Web Application)
4. Database Security
5. Network Integrity
6. Access Controls
7. Backup and Recovery
8. BCP/DR (Only applicable for Depository Participants having BCP / DR site)
9. Segregation of Data and Processing facilities
10. Back-office data
11. User Management
12. IT Infrastructure Management (including use of various Cloud computing models such as Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS))
13. Software Testing Procedures - The system auditor should check whether the depository participants has complied with the guidelines and instructions of SEBI / Depository with regard to testing of software and new patches, including the following:
14. Additional Points
15. AI-ML
16. Asset Management
17. Remote Access Controls
18. SEBI and Depository Compliances
19. ISO Certifications
20. Concentration Risk on Outsourced Agencies:
21. Phishing & Malware Protection for Depository applications/ DP systems
22. Information Risk Management



# Central Depository Services (India) Limited

Convenient + Dependable + Secure

## COMMUNIQUE TO DEPOSITORY PARTICIPANTS

### 6. 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.

Last date of Submission 31-May-2024 . If the report is submitted after this date, then it will be treated as non compliance.

1. SOFTWARE CHANGE MANAGEMENT – THE SYSTEM AUDITOR SHOULD CHECK WHETHER PROPER PROCEDURES HAVE BEEN FOLLOWED AND PROPER DOCUMENTATION HAS BEEN MAINTAINED FOR THE FOLLOWING:

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 Finding
1 (a)	Processing / approval methodology of new feature request, change or patches	COMPLIED	test		15-05-2025	-SELECT-
1(b)	"Change Management process, related approvals, version control history, etc. Change requests: Whether the changes are tested in UAT environment before being approved for deployment into production. Whether the categorization of the change is done properly."	COMPLIED	test		15-05-2025	-SELECT-
1 (c)	Fault reporting / tracking mechanism and process for resolution	NOT COMPLIED	Ak	te	dd-mm-yyyy	-SELECT-
1 (d)	Testing of new releases / patches / modified software / bug fixes	NA	t	te	dd-mm-yyyy	-SELECT-

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

### 7. Fill in all the details in the checkpoint's description.

Last date of Submission 31-May-2024 . If the report is submitted after this date, then it will be treated as non compliance.

1. SOFTWARE CHANGE MANAGEMENT – THE SYSTEM AUDITOR SHOULD CHECK WHETHER PROPER PROCEDURES HAVE BEEN FOLLOWED AND PROPER DOCUMENTATION HAS BEEN MAINTAINED FOR THE FOLLOWING:

2. PASSWORD SECURITY

3. SESSION MANAGEMENT (MOBILE APPLICATION / CLIENT SERVER APPLICATION / WEB APPLICATION)

4.DATABASE SECURITY

5. NETWORK INTEGRITY

6. ACCESS CONTROLS

7. BACKUP AND RECOVERY

8. BCP/DR (ONLY APPLICABLE FOR DEPOSITORY PARTICIPANTS HAVING BCP / DR SITE)

9.SEGREGATION OF DATA AND PROCESSING FACILITIES

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



# Central Depository Services (India) Limited

Convenient + Dependable + Secure

## COMMUNIQUE TO DEPOSITORY PARTICIPANTS

- Now click on "Choose files". Upload the Declaration from the MD/CEO/Partners/Proprietor file & click on 'SAVE' button. **Declaration from the MD/CEO is mandatory.**

### DESIGNATED OFFICER LOGIN

- 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

## COMMUNIQUE TO DEPOSITORY PARTICIPANTS

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

**AUDIT APPLICATION**

**LOGIN OTP**

Enter OTP

OTP Time :- 00:09:56

Do not refresh the page

Verify OTP

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

3. Then select audit type "System Audit Report" from the Drop down.  
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

**AUDIT APPLICATION**

**Reports**

Select Audit Type: SYSTEM AUDIT REPORT

Select Audit Month: March-2024

Select DP / RTA:

Confirm

View Cyber Report | View Compliance | View Resubmission  
Cyber Audit Compliance Report | Cyber RCA Report

View Pending Submission | View Pending Non-Compliance

Go to Login | Change Password

FAQ

FAQ for online submission of SAR | Manual for Online Submission of WCE

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



# Central Depository Services (India) Limited

Convenient + Dependable + Secure

## COMMUNIQUE TO DEPOSITORY PARTICIPANTS

4. The below screen will be displayed once the user is logged in.

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

**AUDIT APPLICATION**

**SYSTEM AUDIT REPORT**

Date: 26-05-2025 16:58:49 DP Name: DP ID: Period: 2023-24

System Audit Report covers the following Branch DPIDs :- 192200

Is the report uploaded on the letter head of CERT-in empanelled entity with DP ID & DP Name specified. YES

Name of CERT-in empanelled entity: test

CERT-in empanelment validity expiry Date (DD-MM-YYYY): 14-05-2025

No of consecutive audits performed by the auditor: 4

Date of Audit Report: 21-05-2025

Last date of Submission 31-May-2024. If the report is submitted after this date, then it will be treated as non compliance.

1. SOFTWARE CHANGE MANAGEMENT – THE SYSTEM AUDITOR SHOULD CHECK WHETHER PROPER PROCEDURES HAVE BEEN FOLLOWED AND PROPER DOCUMENTATION HAS BEEN MAINTAINED FOR THE FOLLOWING:

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

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

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

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

**AUDIT APPLICATION**

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"	-SELECT-			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"	-SELECT-			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."	-SELECT-			dd-mm-yyyy	-SELECT-
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"	-SELECT-			dd-mm-yyyy	-SELECT-

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



# Central Depository Services (India) Limited

Convenient + Dependable + Secure

## COMMUNIQUE TO DEPOSITORY PARTICIPANTS

6. Fill in all the details in the checkpoint's description.

1. SOFTWARE CHANGE MANAGEMENT – THE SYSTEM AUDITOR SHOULD CHECK WHETHER PROPER PROCEDURES HAVE BEEN FOLLOWED AND PROPER DOCUMENTATION HAS BEEN MAINTAINED FOR THE FOLLOWING:

2. PASSWORD SECURITY

3. SESSION MANAGEMENT (MOBILE APPLICATION / CLIENT SERVER APPLICATION / WEB APPLICATION)

4. DATABASE SECURITY

5. NETWORK INTEGRITY

6. ACCESS CONTROLS

7. BACKUP AND RECOVERY

8. BCP/DR (ONLY APPLICABLE FOR DEPOSITORY PARTICIPANTS HAVING BCP / DR SITE)

9. SEGREGATION OF DATA AND PROCESSING FACILITIES

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

7. Upload System Audit Report file and click on declaration.

Click on SAVE Button & 'Submit to CDSL'.

**System Audit report file submission is mandatory before submitting to CDSL.**

ID	Particulars	CRITICAL	HIGH	MEDIUM	low
1	COMPLIED	0	0	0	0
2	NOT COMPLIED	0	0	0	0
3	N/A (Not Applicable)	0	0	0	0
4	Total	0	0	0	0

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

Choose File | No file chosen | Upload | .pdf

Attach File

Choose File | No file chosen | Upload | .pdf

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

Save | Submit to CDSL | Cancel

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



# Central Depository Services (India) Limited

Convenient + Dependable + Secure

## COMMUNIQUE TO DEPOSITORY PARTICIPANTS

---

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

- 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.
- Severity level is mandatory and must be categorized as Critical, High, Medium, or Low.
- The report must be as per the Communique No.CDSL/RISK/DP/POLCY/2024/536 September 16, 2024, in the PDF format only.
- 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 uploading the report/declaration/submitting the form, request you to send an email on [dpinfosec@cdslindia.com](mailto:dpinfosec@cdslindia.com) along with the screenshot of the error.

\*\*\*\*