



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

CDSL/IS/DP/POLCY/2026/401

June 12, 2026

SUBMISSION OF CYBER AUDIT REPORT

Depository Participants (DPs) are advised to refer Circular No. **CDSL/IS/DP/POLCY/2026/347** **May 22, 2026**, regarding the submission of Cyber Security Audit report.

In view of the above, Depository Participants are hereby advised to submit the Cyber Audit Report through the online audit web portal. The deadline for **Cyber Audit** report submission is on or before **30th June 2026**.

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

All Depository Participants are advised to take note of the above and submit all reports or formats related to Cyber Audit from time to time and ensure strict adherence to the compliance requirements.

If the submission is not completed within the prescribed timeline, it will be treated as noncompliance, and the applicable penalty will be imposed as per **CDSL communique no: CDSL/AUDIT/DP/POLCY/2025/105 February 12, 2025**.

Queries regarding this communiqué may be addressed to dpinfosec@cdslindia.com.

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 Cyber Security Audit Report

IT Auditor needs to be mapped before submissions

1. Select "DP" as Login Type. Enter your user id and password. Complete the Captcha and then Sign In.

AUDIT APPLICATION

SIGN IN

Login Type: DP

User ID: [Input Field]

Password: [Input Field]

Captcha: 88ed81

Sign In

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

2. Enter the OTP received on the registered mobile number and email id.

AUDIT APPLICATION

LOGIN OTP

Enter OTP: [Input Field]

OTP Time :- 00:09:45

Do not refresh the page

Verify OTP



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUE TO DEPOSITORY PARTICIPANTS

3. Then click on “View DP / RTA Profile and Status of Reports”.

AUDIT APPLICATION

Select Audit Type	--SELECT--	v
Select Audit Month		v
Select DP / RTA	--Select--	v

Confirm

[View DP / RTA Profile and Status of Reports](#)
[View IT Auditor Profile](#)
[View Auditor Profile](#)

[View Investor Complaints](#)

4. You can view the mapped logins for each login type on this page.

AUDIT APPLICATION

IT Auditor Profile

User ID:	<input type="text"/>
Name of Audit Firm:	<input type="text"/>
Address:	<input type="text"/>
Name of the Auditor:	<input type="text"/>
Mobile:	<input type="text"/>
Email ID:	<input type="text"/>

Update Profile

Back

MAPPED DP WITH AUDIT TYPES

Delete	Edit	DP ID	DP Name	Audit Firm Name	User ID	Mobile No.	Audit Type
Delete	Edit						SYSTEM AUDIT REPORT
Delete	Edit						CYBER SECURITY AUDIT ATR

5. Go back. Click on “Registration for IT Auditor”

AUDIT APPLICATION

Select Audit Type	--SELECT--	v
Select Audit Month		v
Select DP / RTA	--Select--	v

Confirm

[View DP / RTA Profile and Status of Reports](#)
[View IT Auditor Profile](#)
[View Auditor Profile](#)

[View Investor Complaints](#)

[View Pending Submission](#) | [View Pending Non-Compliance](#)

[Go to Login](#) | [Change Password](#)

[Registration for Auditor](#) | [Registration for IT Auditor](#) | [Registration for Designated Officer](#) | [User registration - Bidding DP](#)

[Register Your KYC User Click Here!!!](#)

[Sectoral Risk Assessment](#)



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

6. After Selecting “Registration for IT Auditor” below screen would be displayed.

AUDIT APPLICATION

IT AUDITOR REGISTRATION

Select Audit Type	--Select--	▼
Auditor List	--SELECT--	▼
* Auditors Email ID	<input type="text" value="Email ID"/>	
* Name of Audit Firm	<input type="text" value="Audit Firm Name"/>	
Address of Audit Firm	<input type="text" value="Address"/>	/
* Name of Contact Person	<input type="text" value="Contact Person"/>	
* Mobile No.	<input type="text" value="Mobile no."/>	
Select DP		▼

Register

[Go to Login](#) | [Refresh](#)

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

7. Select “Cyber Security Audit Report” as the Audit Type.
Enter All details like Auditors Email ID, Name of Audit Firm, Name of the contact person, Mobile Number. Select DP. And then click on Register.

AUDIT APPLICATION

IT AUDITOR REGISTRATION

Select Audit Type	CYBER SECURITY AUDIT REPORT	▼
Auditor List	--SELECT--	▼
* Auditors Email ID	<input type="text"/>	
* Name of Audit Firm	<input type="text"/>	
Address of Audit Firm	<input type="text" value="Address"/>	/
* Name of Contact Person	<input type="text"/>	
* Mobile No.	<input type="text"/>	
Select DP		▼

Register

[Go to Login](#) | [Refresh](#)

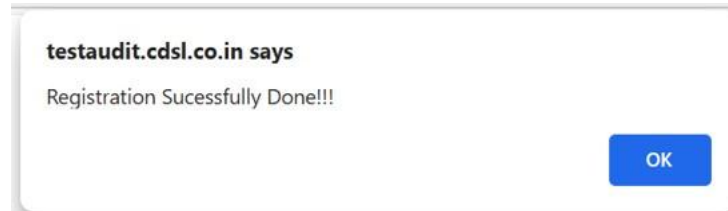


Central Depository Services (India) Limited

Convenient # Dependable # Secure

COMMUNIQUE TO DEPOSITORY PARTICIPANTS

- Once Registration is done, a pop-up box will appear intimating the same.



- Then click on Forgot Password.

AUDIT APPLICATION

SIGN IN

Login Type IT_Auditor

User ID [input field]

Password [input field]

085a24 [refresh icon]

[input field]

Sign In

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

- After Clicking on Forgot Password it will redirect to below screen shot.

AUDIT APPLICATION

FORGOT PASSWORD

Login Type --Select--

User ID User ID

Email ID Email ID

I'm not a robot

Submit **Cancel**



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUE TO DEPOSITORY PARTICIPANTS

11. Select IT Auditor as the Login Type.

Enter User ID and Email ID. Please note that the User ID must be email ID.

Complete captcha verifications and then Submit.

AUDIT APPLICATION

FORGOT PASSWORD

 Login Type	<input type="text" value="IT_Auditor"/>
 User ID	<input type="text"/>
 Email ID	<input type="text"/>
<div style="display: flex; align-items: center; justify-content: center;"><div style="margin-right: 10px;"> I'm not a robot</div><div style="border: 1px solid #ccc; padding: 2px;"> <small>reCAPTCHA Privacy - Terms</small></div></div>	
<div style="display: flex; justify-content: space-around;">SubmitCancel</div>	

12. Enter the OTP received on the registered number or email id

AUDIT APPLICATION

FORGOT PASSWORD

 **Enter OTP**

OTP Time :-
00:09:12

Do not refresh the page
Verify OTP

13. Enter New password and confirm the new password. Click on Save Changes.

AUDIT APPLICATION

FORGOT PASSWORD

You can reset your password here

 **New Password**

 **Confirm Password**

Save Changes

* Password Instructions : At least one digit [0-9], one lowercase character [a-z], one uppercase character [A-Z], one special character [*.!@#\$%^&(){}[];:<>.,] and at least 8 characters in length



Central Depository Services (India) Limited


Convenient + Dependable + Secure


COMMUNIQUE TO DEPOSITORY PARTICIPANTS


14. After resetting password, Login as an IT Auditor.


AUDIT APPLICATION

SIGN IN

 **Login Type**

 **User ID**

 **Password**

a55ad5 

Sign In

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

15. You will receive the OTP on the registered mobile number and email id.

testaudit.cdsl.co.in says


OTP sent successfully on your registered email id / Mobile...!!!

OK

16. Enter the OTP to Login

AUDIT APPLICATION

LOGIN OTP

 **Enter OTP**

OTP Time :-
00:09:42

Do not refresh the page

Verify OTP



Central Depository Services (India) Limited

Convenient # Dependable # Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

IT AUDITOR LOGIN

1. Log in Into Audit application by using the below link:
<https://auditweb.cdslindia.com/Login.aspx>

Now Sign in using 'Login Type-IT Auditor'.

Now enter User ID & Password and click on "Sign In" button.



SIGN IN

Login Type	IT_Auditor
User ID	Enter Login ID
Password	Password
	daff8f
	Enter Code
Sign In	
Forgot password	Registration for DP / RTA

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



LOGIN OTP

Enter OTP	Enter OTP
OTP Time :- 00:09:25	Do not refresh the page
Verify OTP	



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**’.

AUDIT APPLICATION

Select Audit Type	CYBER SECURITY AUDIT REPORT	▼
Select Audit Month		▼
Select DP / RTA	--Select--	▼
Confirm		
View Pending Submission View Pending Non-Compliance		
Go to Login Change Password		

- Select the DP category

Please note that once the DP Category is selected, it cannot be changed.

AUDIT APPLICATION

Please Note: Once the DP category is selected, it cannot be changed.

* Select DP Category	--Select--
----------------------	------------

- Please select the appropriate DP category from the options listed below.

AUDIT APPLICATION

* Select Category	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #f0f0f0; padding: 2px;">--Select--</div> <div style="background-color: #f0f0f0; padding: 2px;">--Select--</div> <div style="background-color: #0056b3; color: white; padding: 2px;">Qualified REs</div> <div style="padding: 2px;">Mid-size REs (providing IBT or Algo trading as Stockbroker)</div> <div style="padding: 2px;">Mid-size REs (not providing IBT or Algo trading as Stockbroker)</div> <div style="padding: 2px;">Small-size REs (providing IBT or Algo trading as Stockbroker)</div> <div style="padding: 2px;">Small-size REs (not providing IBT or Algo trading as Stockbroker)</div> <div style="padding: 2px;">Rest of the RE</div> </div>
-------------------	--

- If the DP categorised itself as **Self-Certified RE**, then the DP is not eligible for the half yearly cyber audit submission.

- DPs are permitted to upload the “**Auditor’s Certificate**” on the auditor’s letterhead, in accordance with Circular No. CDSL/OPS/DP/POLCY/2024/468 dated August 21,2024, under the CSCRF – Annexure P (Reporting Format for Self-Certification for REs) and submit it to CDSL.

AUDIT APPLICATION

Please Note: Once the DP category is selected, it cannot be changed.

* Select DP Category	Self Certified RE
Since you have categorised yourself as Self Certified RE, you are not eligible for the half yearly cyber audit submission.	
Auditor Certificate	<div style="display: flex; align-items: center; gap: 10px;"> <div style="border: 1px solid #ccc; padding: 2px;">Choose File</div> <div style="color: #ccc;">No file chosen</div> <div style="background-color: #0056b3; color: white; padding: 2px 5px; border-radius: 3px;">File Upload</div> <div style="background-color: #0056b3; color: white; padding: 2px 5px; border-radius: 3px;">Submit To CDSL</div> <div style="background-color: #c00; color: white; padding: 2px 5px; border-radius: 3px;">Back</div> </div>



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

7. Please note that all DPs, except **Self-Certified REs**, are required to follow the complete Cyber Audit submission process.

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.

8. Please ensure that all necessary details specified in the Terms of Reference (TOR) for the Cyber Security Audit Report, as outlined in Communique No: **CDSL/IS/DP/POLCY/2026/347 May 22, 2026**, are duly entered.

Checkpoints Description:

1. Governance
2. Identification
3. Protection
4. Risk Management
5. Physical Security
6. Access Control
7. Network Security Management
8. Data Security
9. Hardening of Hardware and Software
10. Application Security in Customer Facing Applications
11. Patch Management



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

12. Disposal of Data, Systems and Storage Devices
13. Vulnerability Assessment and Penetration Testing (VAPT)
14. Monitoring and Detection
15. Response and Recovery
16. Sharing of Information
17. Training and Education
18. Systems Managed by Vendors
19. SEBI and Exchange/Depositories Compliances, Advisory for Financial Sector Organizations
20. Cyber Security Advisory - Standard Operating Procedures (SOP)
21. Security of Cloud Services
22. Concentration Risk on Outsourced Agencies
23. Certification of Off-The-Shelf Products
24. Compliance status of last inspection carried out by SEBI/ Depository

9. Please provide the following details

The screenshot shows a web-based form titled "AUDIT APPLICATION". At the top, there is a blue header with the text "AUDIT APPLICATION". Below the header, there is a yellow warning box that says "Please Note: Once the DP category is selected, it cannot be changed." Below this, there is a dropdown menu for "Select DP Category" with the option "Mid-size REs (not providing BT or Algo trading as Stockbroker)" selected. The main form is titled "CYBER SECURITY AUDIT REPORT" and contains several fields: "Date" (04/06/2020 12:18), "DP Name", "DP ID", and "Period" (April 2015 - March 2020). There is a section for "Cyber Audit Report covers the following Branch DPIDs:-" with a "Submit" button. Below this, there are several checkboxes and text boxes: "Is the report uploaded on the letter head of CERT in empaneled entity with DP ID & DP Name specified." (YES), "Name of CERT in empaneled entity:" (Text box), "CERT in empaneled entity expiry date (DD-MM-YYYY):" (29-09-2020), "No of consecutive audits performed by the auditor:" (0), and "Date of Audit Report:" (01-06-2020). A red warning message states: "If the report is not submitted within prescribed timeline, it will be treated as non-compliance & applicable penalty would be imposed". At the bottom, there is a section titled "AUDITOR'S DECLARATION" with a "DECLARATION" button and four sub-sections: "1. GOVERNANCE", "2. IDENTIFICATION", "3. PROTECTION", and "4. RISK MANAGEMENT".



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

10. Click on the Declaration section and enter the required information.

DECLARATION

TO WHOM SO EVER IT MAY CONCERN

This is to declare and certify that I am a Partner/Proprietor of firm _____ with CERT-In empanelment from _____ to _____ I have conducted Cyber audit for _____ period as per the requirements of SEBI.

Checklist for Cyber audit as required :

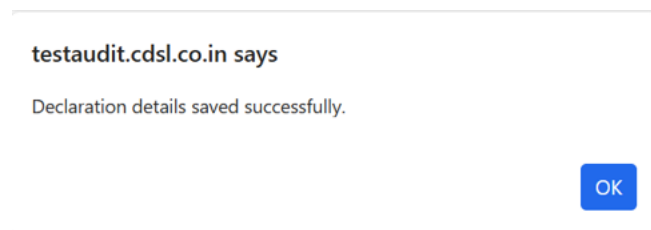
Sr. No	Area	Details of the audit area	Is the Entity Compliant? (Yes/No)	Auditor's comments
1.	Cybersecurity and Cyber resilience policy		-select-	
2.	Asset Inventory		-select-	
3.	Risk assessment and Risk management		-select-	
4.	Supply chain risk management		-select-	
5.	Awareness and Training		-select-	

11. Fill in all the required information in the Declaration section and click the **Save** button at the bottom of the page.

5. Summary of findings (Including identification tests, tools used, and results of tests performed)

Sr. No	Number of Non-conformity / Observations	Risk rating				Any other comments
		Critical	High	Medium	Low	
No records found						

12. After saving the segment, the message shown below will appear. Please ensure that you click the **Save** button after completing each segment.





Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

13. Open each segment of the TOR and fill the required information.

The 'IT Auditor' is given access to fill only the below mentioned fields:

- Description of Finding(s)/ Observation(s)
- Name of the system belongs to RE or third-party vendor
- Status (Complied/Non-complied/Not Applicable)
- Risk rating (C/H/M/L) of the findings
- C//A affected
- Test cases used
- Root Cause Analysis
- Impact analysis
- Auditor recommendations/ Corrective actions
- List of documentary evidence including physical inspection/ sample size taken by the auditor
- Whether similar issue was reported in the last three audits

Please Note Once the IP category is selected, it cannot be changed.

* Select IP Category [Click here to understand IP or Audit type in Detail](#)

*Date of Audit Report: EOL: 2024

*This report is not submitted within prescribed timeline, it will be treated as non-compliance if applicable penalty would be imposed

AUDITOR'S DECLARATION

DECLARATION

1. GOVERNANCE

No.	Standards prescribed by ISB /ISCR/	Details	Description of Finding/ Observation/Process only the ISB/ISCR to be used applicable to the IP	Name of System/ Vendor to RE or third party vendor	Number/Name of Finding	Risk Rating of the Finding	C/D/A affected	Test Cases Used	Root Cause Analysis	Impact Analysis	Auditor's recommendation/Corrective actions	Timeline of corrective actions	Management Response	Whether similar issue was reported in the last three audits	List of documentary evidence including physical inspection/ sample size taken by the auditor
101	ISCR022	Has the RE established an audit effort or audit observation security (OAS) which would result in timely, identify and report observation, take action to resolve, establish appropriate controls and controls, and drive the establishment and maintenance of practice and procedure in case the observation and other evidence only approved by the Board/Chief Auditor of the RE. In the reporting of the OAS only to the MD or CEO of their organization? Does the OAS ensure sufficient qualifications and capabilities to carry out their responsibilities? Has the RE established a reporting procedure to facilitate communication of observation/ incident/ or audit activities to the CEO or to the senior management in a time bound manner as defined by governance/audit/ internal regulations etc. for the best, guide, and reporting of the OAS on best reputation to the CEO?				SELECT	SELECT	SELECT						SELECT	
102	ISCR023	Has the RE established an audit effort or management observation (MO) which would result in timely, identify and report observation, take action to resolve, establish appropriate controls and controls, and driving the development and maintenance of practice and procedure in case the observation and other evidence only approved by the Board/Chief Auditor of the RE. Has the RE established a reporting procedure to facilitate communication of observation/ incident/ or audit activities to the CEO or to the senior management in a time bound manner as defined by governance/audit/ internal regulations etc. for the best, guide, actions, fees, structure or regulation?				SELECT	SELECT	SELECT						SELECT	
103	ISCR024	Has the RE established an adequate control log of the audit/ finding by identifying/Has the observation been raised under a case management system according to the best of practices or best management?				SELECT	SELECT	SELECT						SELECT	



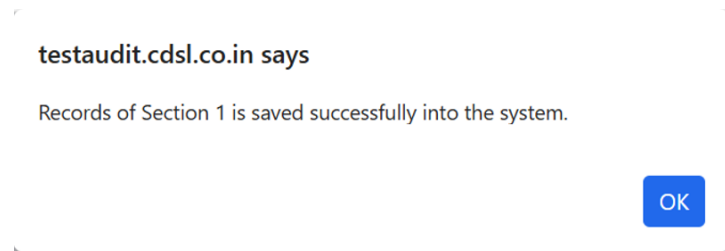
Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

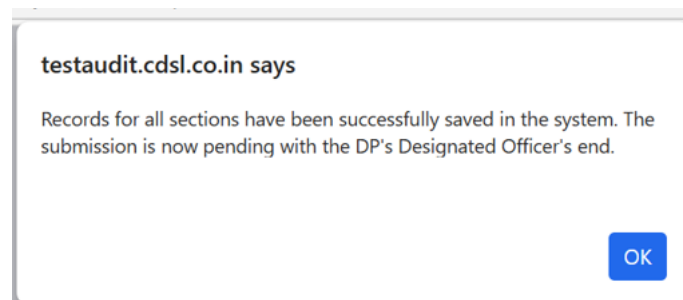
14. Open each section and fill in the required information. After completing a section, click the **“Save”** button to save the details.

15. Once the segment has been saved, the following message will be displayed. Kindly note that the **“Save”** button must be clicked after each segment.



16. After completing all the required information in each segment and saving every segment individually, click the **“Save & Submit to DP”** button.

17. If all mandatory fields have been completed correctly, the popup shown below will appear, and the submission will be pending at the Designated officer end for further action. If any errors are present, they will be displayed at the bottom of the report.





Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ 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.

AUDIT APPLICATION

SIGN IN

Login Type: Designated Officer

User ID: Enter Login ID

Password: Password

2d7b48

Enter Code

Sign In

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

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

AUDIT APPLICATION

LOGIN OTP

Enter OTP: Enter OTP

OTP Time :- 00:09:47

Do not refresh the page

Verify OTP



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUE TO DEPOSITORY PARTICIPANTS

- Then select audit type **“Cyber Security Audit Report”** 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 REPORT	▼
Select Audit Month	March-2026	▼
Select DP / RTA	--Select--	▼

Confirm

- The details entered by the auditor will be displayed on the screen.

AUDIT APPLICATION

Please Note: Once the DP category is selected, it cannot be changed.

* Select DP Category Qualified REs ▼

CYBER SECURITY AUDIT REPORT

* Date	10/06/2026 16:58	* DP Name	
* DP ID		* Period	

Cyber Audit Report covers the following Branch DPIDs :-

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

*** Name of CERT-in empanelled entity :** Text Firm

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

*** No of consecutive audits performed by the auditor:**

*** Date of Audit Report:**

If the report is not submitted within prescribed timeline, it will be treated as noncompliance & applicable penalty would be imposed

- Open each segment of the TOR and fill the required information.
The **‘Designated Officer’** is given access to fill only the below mentioned fields:

- Deadline of corrective action(s)
- Management response

* Select DP Category Qualified REs ▼

This report is not submitted within prescribed timeline. It will be treated as noncompliance & applicable penalty would be imposed

AUDITOR'S DECLARATION

DECLARATION

1. GOVERNANCE

Sl. No.	SIR/CSRF	Details	Description of Finding/ Observation/Reason why the TOR Clause is not applicable to the DP	Name of Branch/Entity	Introduction of the Finding	Risk Rating of the Finding	CISR Effect	Test Cases Used	Root Cause Analysis	Impact Analysis	Auditor Recommendation/Action Plan	Deadline of corrective action	Management Response	Whether action taken reported in the last 30 days	List of Accountancy entries including planned corrective actions sample size taken by the auditor
161	DP-RE-23	Has the RE designated a senior official as Chief Information Security Officer (CISO) whose function would be to assess, identify and control information risks, respond to security incidents, coordinate incident response activities, and direct the development and implementation of processes and procedures to plan for cyber risks and cyber incident early response by the Branch/Member/Registrar of the RE? Is the reporting of the CISO made to the RE/CSRF in a timely manner? Has the CISO been qualified and certified by any and/or other regulatory bodies in accordance with the regulatory requirements of the CISO as the senior management in a firm based on an external or internal audit conducted by the auditor? Has the RE established a robust framework to ensure the CISO is able to manage the firm based on an external or internal audit conducted by the auditor? Has the RE established a robust framework to ensure the CISO is able to manage the firm based on an external or internal audit conducted by the auditor?													
162	DP-RE-23	Has the RE appointed a senior official or management personnel (the Designated Officer) responsible for assessing, identifying and controlling information risks, responding to security incidents, coordinating incident response activities, and directing the development and implementation of processes and procedures to plan for cyber risks and cyber incident early response by the Branch/Member/Registrar of the RE? Has the reporting of the Designated Officer made to the RE/CSRF in a timely manner? Has the Designated Officer been qualified and certified by any and/or other regulatory bodies in accordance with the regulatory requirements of the Designated Officer as the senior management in a firm based on an external or internal audit conducted by the auditor? Has the RE established a robust framework to ensure the Designated Officer is able to manage the firm based on an external or internal audit conducted by the auditor? Has the RE established a robust framework to ensure the Designated Officer is able to manage the firm based on an external or internal audit conducted by the auditor?													
163	DP-RE-23	Has the RE allocated an adequate percentage of the total IT budget to cybersecurity? Has the allocation been based on a risk-based approach? Has the RE established a robust framework to ensure the allocation is based on a risk-based approach? Has the RE established a robust framework to ensure the allocation is based on a risk-based approach?													



Central Depository Services (India) Limited

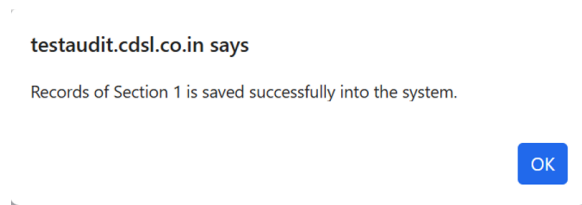
Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

- Open each section and fill in the required information. After completing a section, click the “Save” button to save the details.

The screenshot shows a web form with a table at the top. The table has two columns: 'ID' and 'Description'. The first row has '101' in the ID column and a detailed description of a cyber resilience testing process. Below the table is a 'Save' button. At the bottom of the form are five navigation tabs: '2. IDENTIFICATION', '3. PROTECTION', '4. RISK MANAGEMENT', and '5. PHYSICAL SECURITY'. The '2. IDENTIFICATION' tab is currently selected.

- If all mandatory fields have been completed correctly, the popup shown below will appear.



- After saving all segments, please complete the RE declaration.

The screenshot shows a form titled 'EVENT AUDIT REPORT FOR COMPLIANCE SUBMISSION'. It contains several sections: 'NAME OF THE ORGANIZATION', 'SAFETY TYPE', 'SAFETY CATEGORY', 'REGULATORY FUNCTION', 'NAME OF THE AUDITING ORGANIZATION', 'NAME OF THE REGULATORY', and 'REGISTRATION'. There are also checkboxes for 'Approved' and 'Not Approved' for each section. At the bottom, there are buttons for 'Save & Continue' and 'Cancel & Exit'.

- After completing all the details in the RE declaration, upload the MOM.

A file upload field with the text: '* Minutes of the Meeting (MoM) of IT Committee' in which the Cyber Audit report was approved'. There is a 'Choose File' button, the text 'No file chosen', and an 'Upload' button.

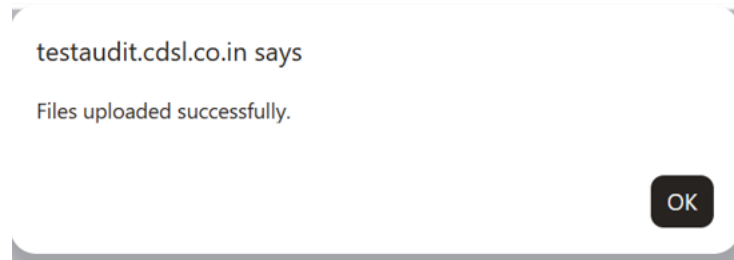


Central Depository Services (India) Limited

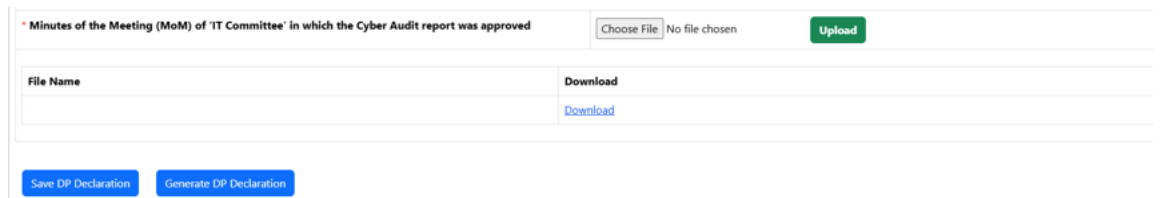
Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

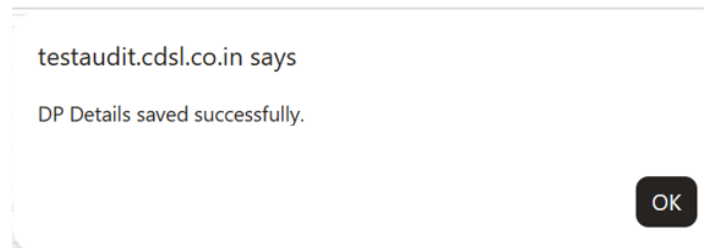
10. After uploading the MOM, the popup shown below will appear.



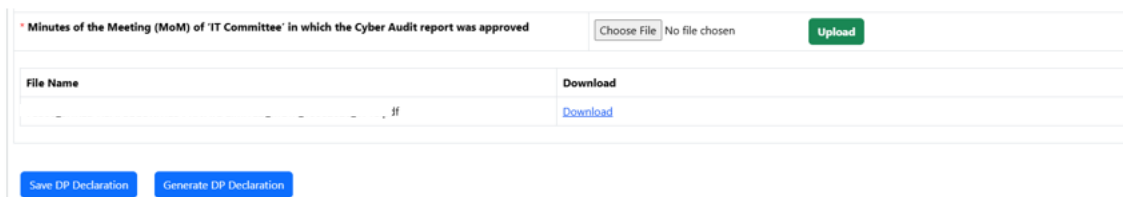
11. After uploading the MOM, click the “Save DP Declaration” button.



12. After saving the DP Declaration, the popup shown below will appear.



13. After saving the DP Declaration, click the “Generate DP Declaration” button. The declaration will be downloaded, as shown in the screenshot below.





Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

14. Your DP Declaration will be downloaded.

The screenshot shows a web form for generating a DP Declaration. At the top, there is a note: "Please Note: Once the DP category is selected, it cannot be changed." Below this, there are several sections for uploading documents: "Select DP Category" (with a dropdown for "Qualified REs"), "Minutes of the Meeting (MoM) of IT Committee" (with a "Choose File" button and "No file chosen" text), and "Attach the Cyber Security Audit Report, duly digitally signed by the auditor." (with a "Choose File" button and "No file chosen" text). A "Downloads" popup is visible in the top right corner, showing a file named "CyberAuditDeclaration_202603_7" with an "Open file" link. At the bottom of the form, there are buttons for "Save", "Generate Auditor Report", "Submit to CDSL", and "Back".

15. After downloading the DP Declaration, attach the digital signature of the MD/CEO/Proprietor/ Partners and upload it in the section mentioned below.

The screenshot shows a section for uploading the RE Declaration. It includes a "Choose File" button and "No file chosen" text, followed by an "Upload" button. Below this, there are instructions: "Please attach the RE's Declaration, duly digitally signed by the MD/CEO/Board member/Partners/Proprietor." and "Kindly ensure that: 1. The first page of the declaration is printed on the RE's official letterhead. 2. The declaration contains the valid digital signature of the MD/CEO/Board member/Partners/Proprietor, as this is mandatory."

16. After uploading the RE Declaration, the popup shown below will appear.



17. Click the "Generate Auditor Report" button.

The screenshot shows the same form as in step 15, but with the "Generate Auditor Report" button highlighted. The "Attach the Cyber Security Audit Report" section is visible, along with the "Declaration" checkbox and the "Generate Auditor Report" button.

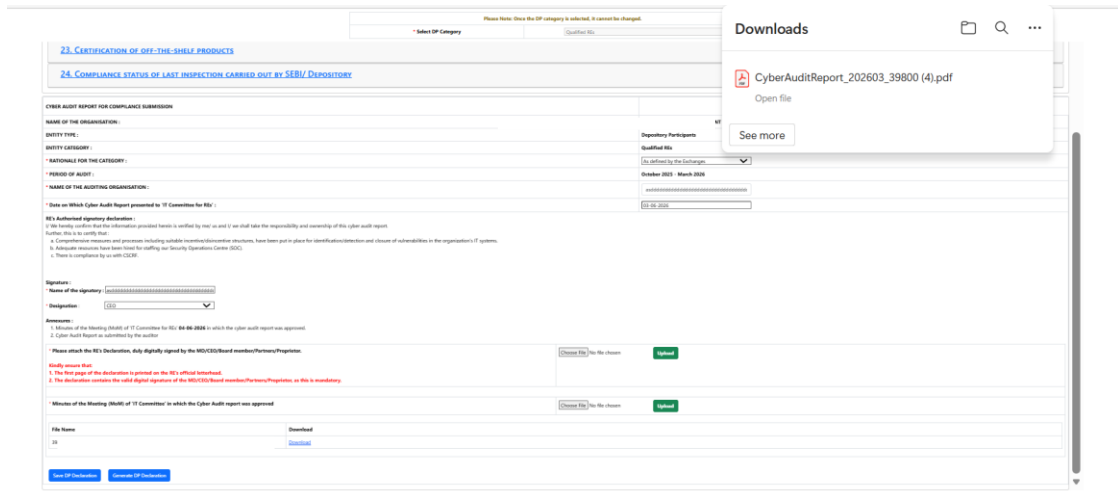


Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

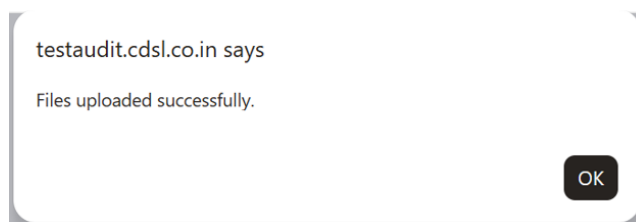
18. Your Cyber Security Audit Report will be downloaded.



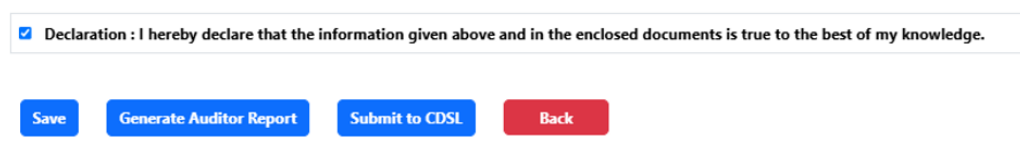
19. After downloading the Cyber Security Audit Report, attach the digital signatures of the Auditor and DP, and upload it in the section mentioned below.



20. After uploading the RE Declaration, the popup shown below will appear.



21. Then select the Declaration checkbox and click the "Save" button.



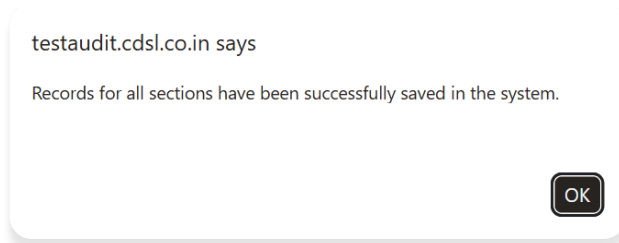


Central Depository Services (India) Limited

Convenient # Dependable # Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

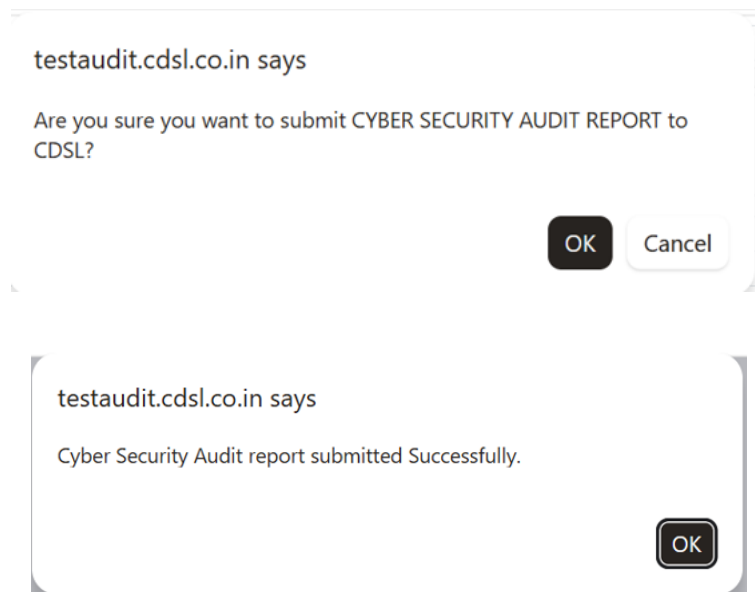
22. After saving the details, the popup shown below will appear.



23. Then click the “**Submit to CDSL**” button.



24. After clicking the “Submit to CDSL” button, the popup shown below will appear, confirming that your submission is complete.





Central Depository Services (India) Limited

Convenient † Dependable † Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

DPs are advised to take note of the following:

- For Self-Certified REs, the “**Auditor’s Certificate**” must be issued on the auditor’s letterhead, in accordance with Circular No. CDSL/OPS/DP/POLCY/2024/468 dated August 21,2024, under the CSCRF – Annexure P (Reporting Format for Self-Certification for REs).
- If any clause under the checkpoint description is marked as “**Complied,**” the auditor must provide the corresponding Status (Complied/Not Complied/Not Applicable) along with a list of documentary evidence reviewed, including details of any physical inspections conducted and the sample size considered during the audit **will be mandatory**.
- If any clause under the checkpoint description is marked as “**Not Complied**” then Description of Finding(s)/ Observation(s), Name of the system belongs to RE or third-party vendor, Status(Complied/Not Complied/Not Applicable), Risk rating (C/H/M/L) of the findings, C//A affected, Test cases used, Root Cause Analysis, Impact analysis, Auditor recommendations/ Corrective actions, Whether similar issue was reported in the last three audits &) along with a list of documentary evidence reviewed, including details of any physical inspections conducted and the sample size considered during the audit.,Deadline of corrective action(s) & Management response **will be mandatory**.
- If any clause under the checkpoint description is marked as marked as “**Not Applicable**” the fields for Description of Finding(s)/ Observation(s) & ‘Management Response along with a list of documentary evidence reviewed, including details of any physical inspections conducted and the sample size considered during the audit **will be 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/Files must be as per the Communique No. **CDSL/IS/DP/POLCY/2026/347 May 22, 2026**, in the PDF format only. **Please rename the file as :DP ID_DP Name_Name of the Report/File_Date (dd/mm/yyyy) it will be file upload date.**
- 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/file, request you to send an email on dpinfosec@cdslindia.com along with the screenshot of the error.