CDSL/AUDIT/DP/POLCY/2021/302 **July 9, 2021**

SUBMISSION OF ANNUAL SYSTEM AUDIT REPORT, INCIDENT/ QUARTERLY REPORTING OF CYBER-ATTACKS, THREATS AND REPORTING OF ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML) APPLICATION AND SYSTEMS USED BY DPS

Reference is drawn to the following SEBI Circulars mentioned in **Table I** below:

Table I:

SEBI Circular Date	SEBI Circular No.	Subject
December 03, 2019 and October 15, 2019	SEBI/HO/MIRSD/CIR/PB/2018/147 SEBI/HO/MIRSD/DOP/CIR/P/2019/109	Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants and its Clarification
January 04, 2019	SEBI/HO/MIRSD/DOS2/CIR/P/2019/10	Reporting for Artificial Intelligence (AI) and Machine Learning (ML) applications and systems offered and used by market intermediaries

As per the above SEBI Circulars, following reports as mentioned in **Table II** are required to be submitted by the DPs to CDSL.

Table II:

Report	Periodicity/ Frequency	Format	Due Date for submission by DP
Reporting of Cyber-attacks, threats	Immediately on occurrence of the incident and Quarterly	Format prescribed in SEBI Circular	15 days after expiry of the quarter
System Audit Report	Annually	Checklist points given in SEBI Circular	3 months from the end of Financial year
Reporting for Artificial Intelligence (AI) and Machine Learning (ML) applications and systems by market intermediaries	Quarterly	Checklist points given in SEBI Circular	15 days after expiry of the quarter

For Cyber incident and AI & ML report, following is the submission schedule.

Schedule Month	Quarter Period	Last Date of Submission
March	Apr – Jun	15-Jul
June	Jul – Sep	15-Oct
September	Oct – Dec	15-Jan
December	Jan – Mar	15-Apr

SEBI has vide circular no. SEBI/HO/MIRSD/DOP/P/CIR/2021/559 dated April 29, 2021 granted relaxation in timeline for Reporting for Artificial Intelligence (AI) and Machine Learning (ML) applications and for submission of Annual System Audit Report for 31st March 2021 till 31st July 2021.

The Manual for submission of the reports as mentioned in Table II above is enclosed as **Annexure A – Manual**

Queries, if any, regarding this communiqué may be addressed to CDSL-Audit: (022) 2305 8679 / 8678/ 8515 or 8513.

sd/-

Latha Nair
Assistant Vice President – Audit, Inspection & Compliance

Manual for Submission of Annual System Audit Report, Incident/ Quarterly reporting of Cyber-attacks, threats and Reporting of Artificial Intelligence (AI) and Machine Learning (ML) application and systems used by DPs

DPs are required to access the CDSL AuditWeb https://auditweb.cdslindia.com/Login.aspx

The DP can login into the same by using their Login credentials.

After logging in, the DP is required to create 2 user login i.e. **DP_IT_Official** and **CISA_Auditor.** (Ref Fig. 1.1)

Fig 1.1

<u>For DP IT Official</u> – The User ID will be

DPID + "_" + All characters before "@" of email ID of the user. Eg: **<u>89900_vikasd</u>** (vikasd@cdslindia.com) (Ref Fig. 1.2)

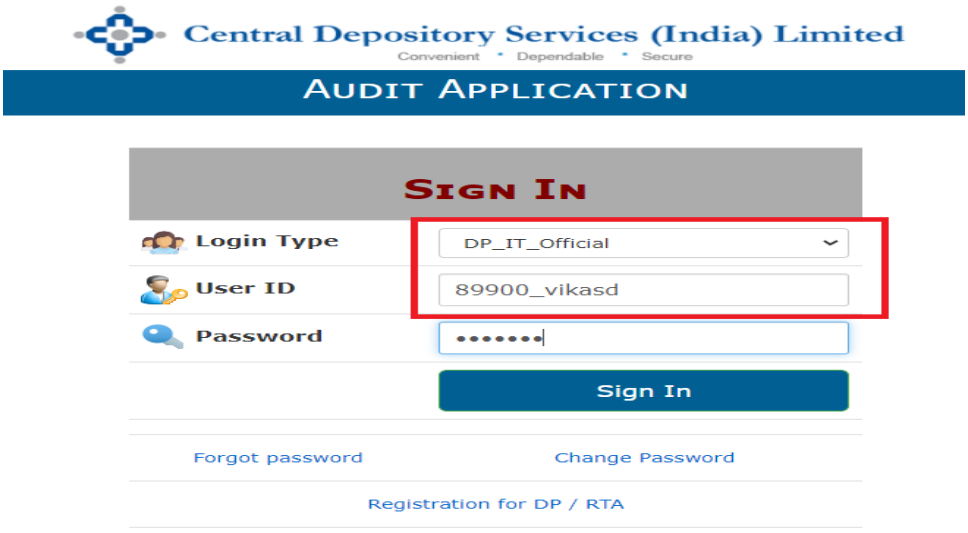


Fig 1.2

For CISA Auditor – The User ID will be

"CISA_" + All characters before "@" of email ID of the user. Eg: **CISA_vikasd** (vikasd@cdslindia.com). (Ref Fig. 1.3)

Different 2 logins are introduced in system

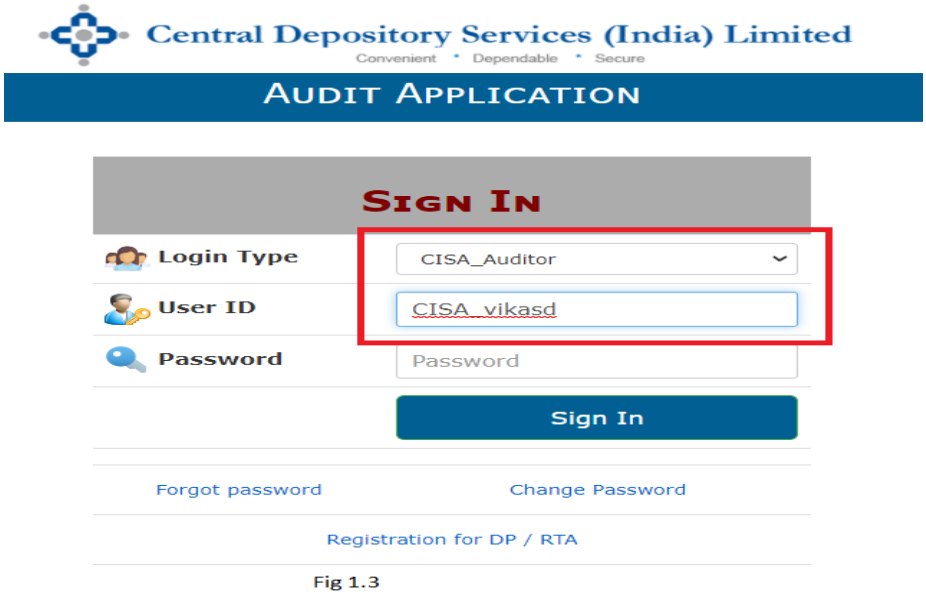


Fig 1.3

DP IT Official / CISA Auditor registration form

Fig 1.4

Fig 1.5

Forgot Password – To get password, click on Forgot password.

Fig 1.6

The Password will be emailed to the registered email ID of the User.

Change Password

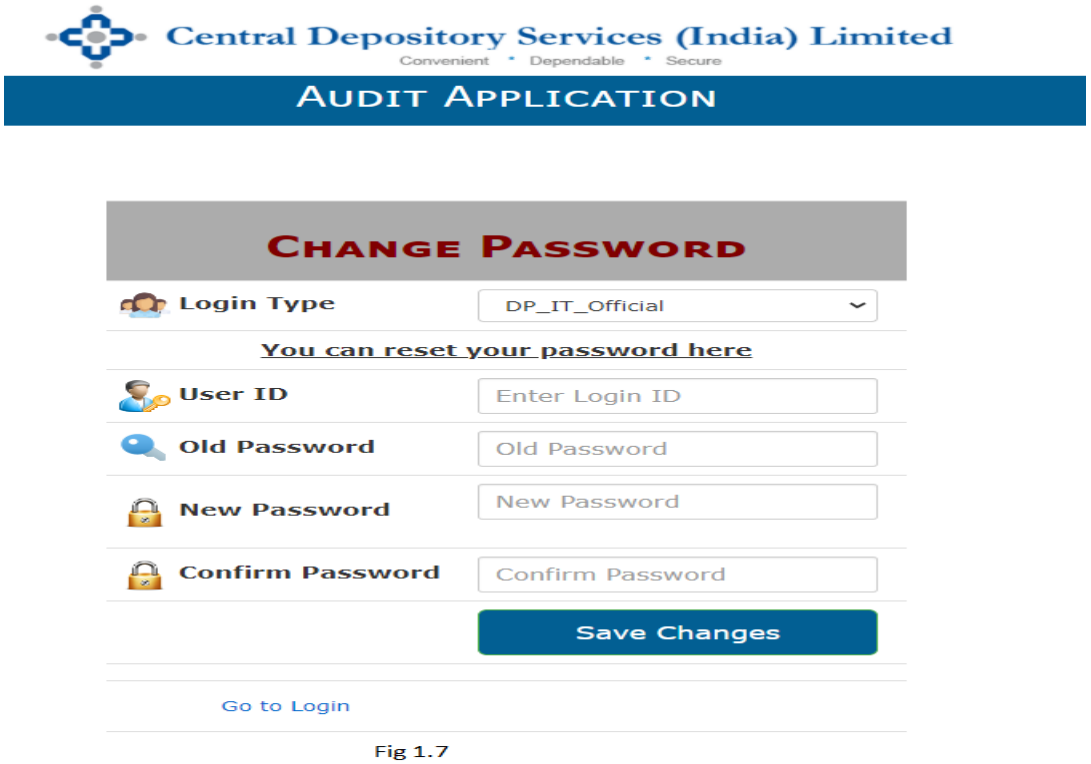


Fig 1.7

Submission of Annual System Audit Report

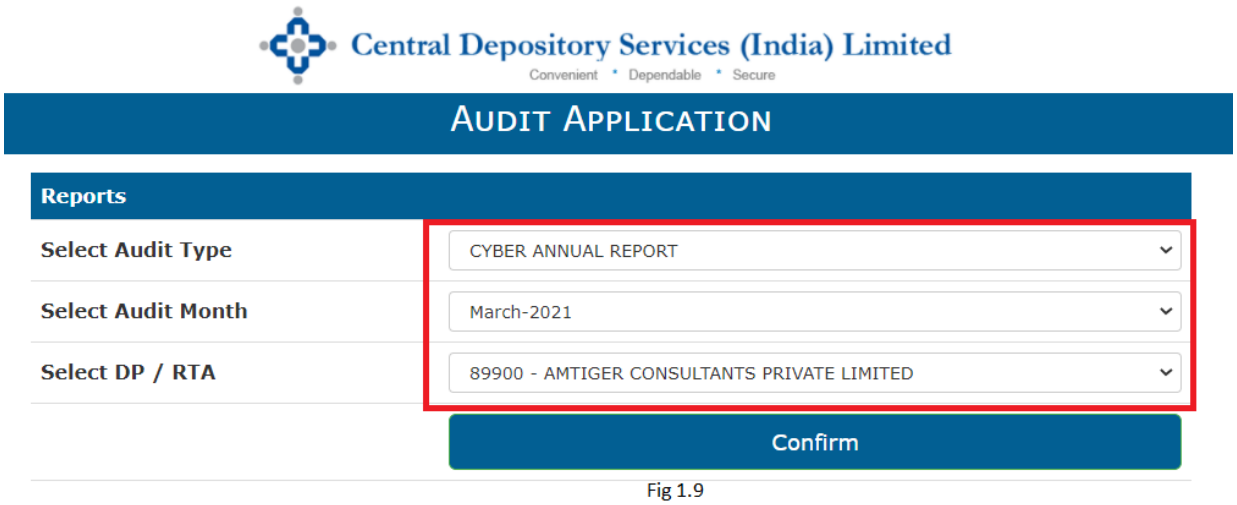


Fig 1.9

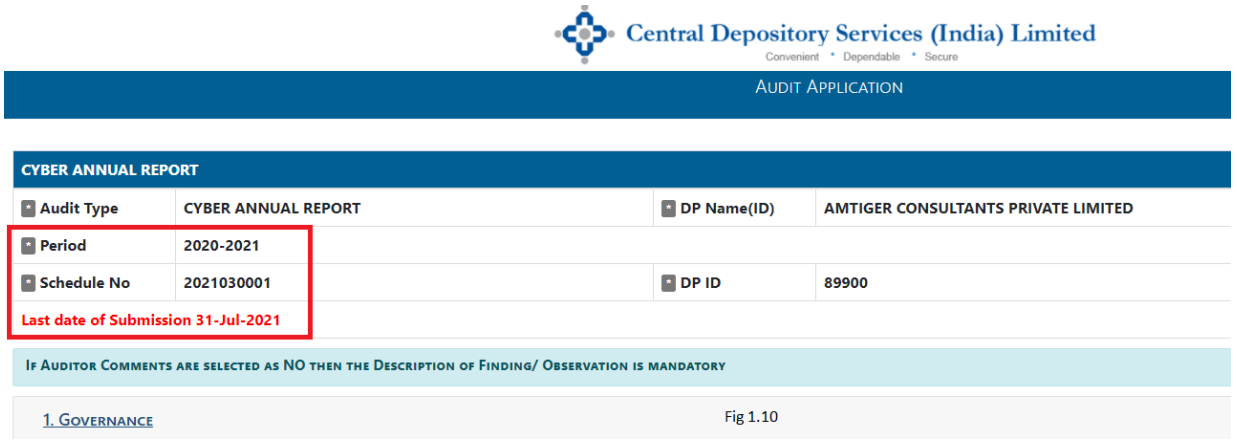


Fig 1.10

- In Cyber annual report. All sections are divided into separate section as per given report format of SEBI-Annual report. (Ref Fig 1.11)
- System have provision to Save the Cyber annual report section wise either DP_IT_Official save the details section wise or to save entire details on one click.
- As per requirement, If Auditor Comments are selected as "NO" by DP_IT_Official then the Description of Finding/ Observation is mandatory. System allows 750 characters.
- CISA_Auditor needs to fill-up management comments If Auditor Comments are selected as "NO" by DP_IT_Official.

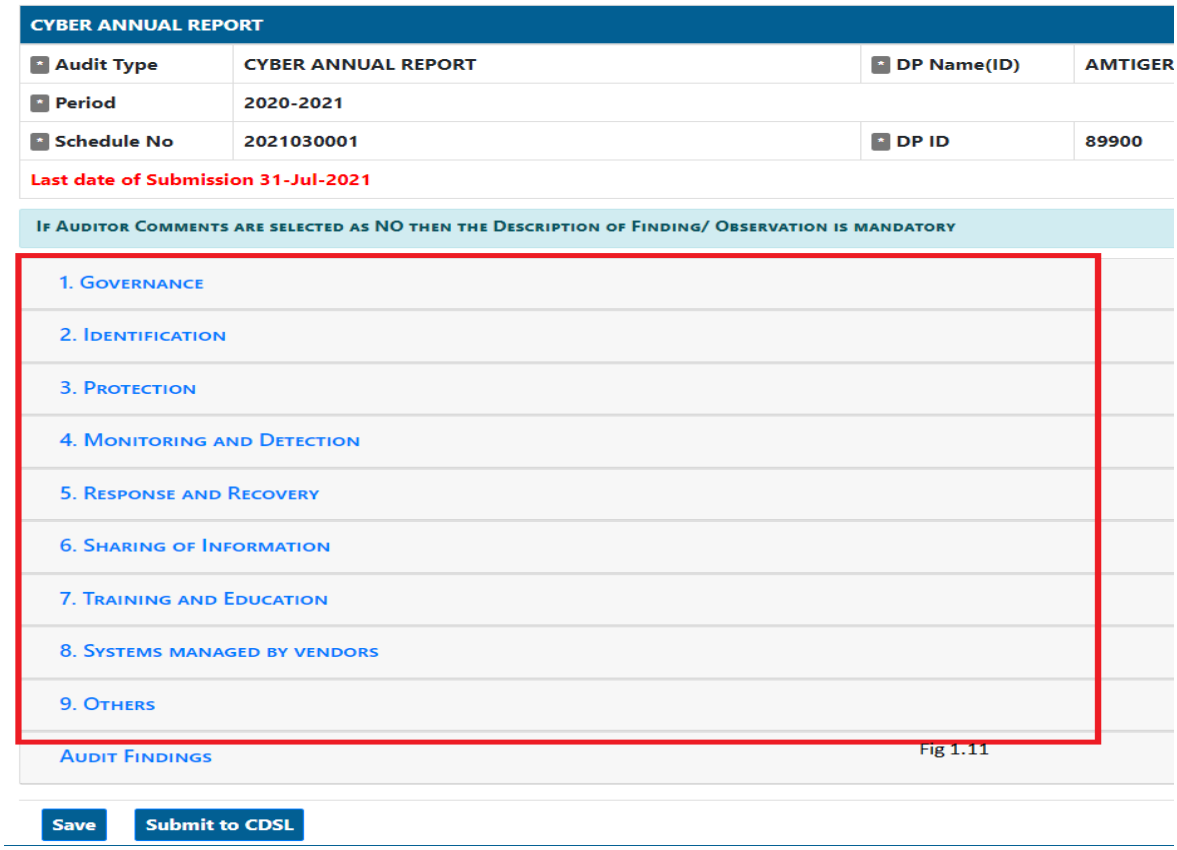
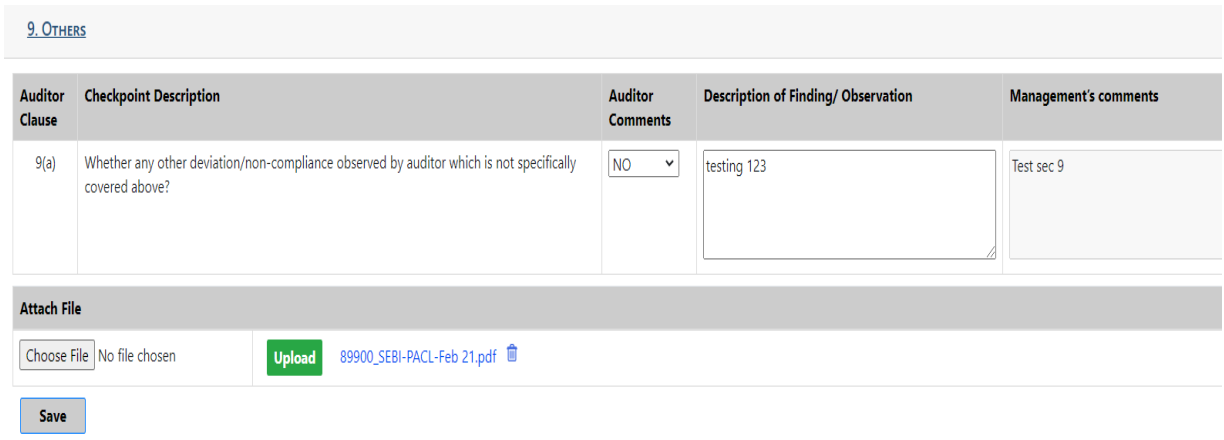
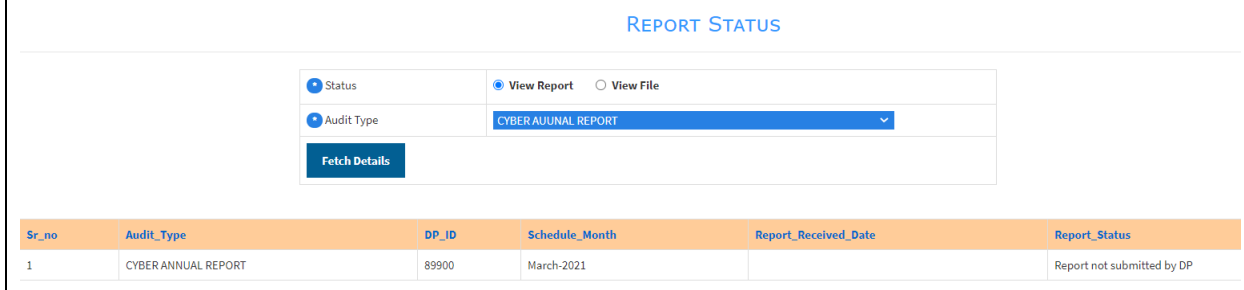


Fig 1.11



- DP_IT_Official needs to upload Annual report. If DP_IT_Official tries to submit the report to CDSL without attaching annual report then system will not allow to submit the report.

Cyber Annual report status



Sr_no	Audit_Type	DP_ID	Schedule_Month	Report_Received_Date	Report_Status
1	CYBER ANNUAL REPORT	89900	March-2021		Report not submitted by DP

Reporting for Artificial Intelligence and Machine Learning

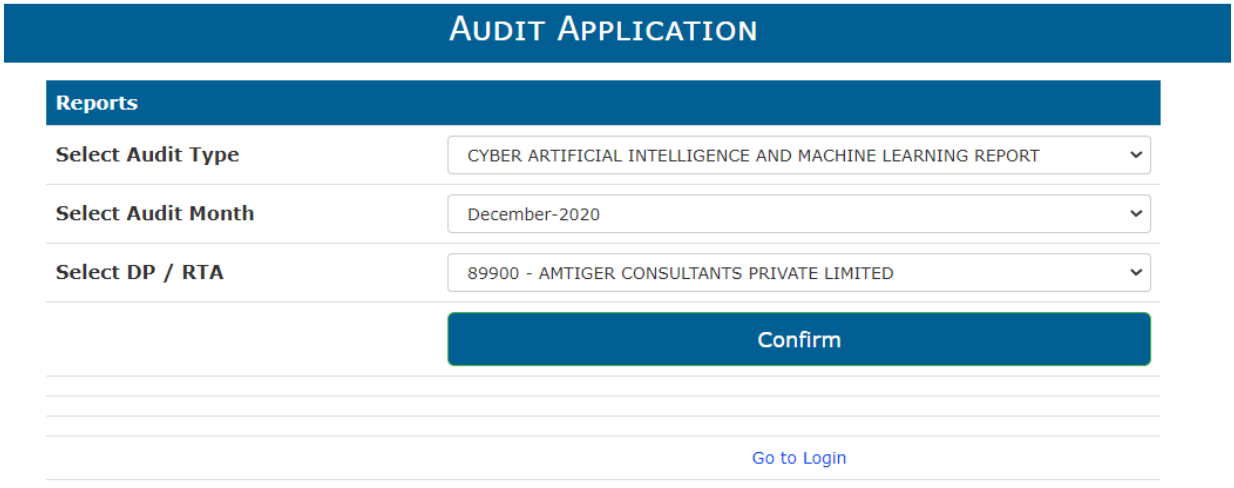


Fig 1.9

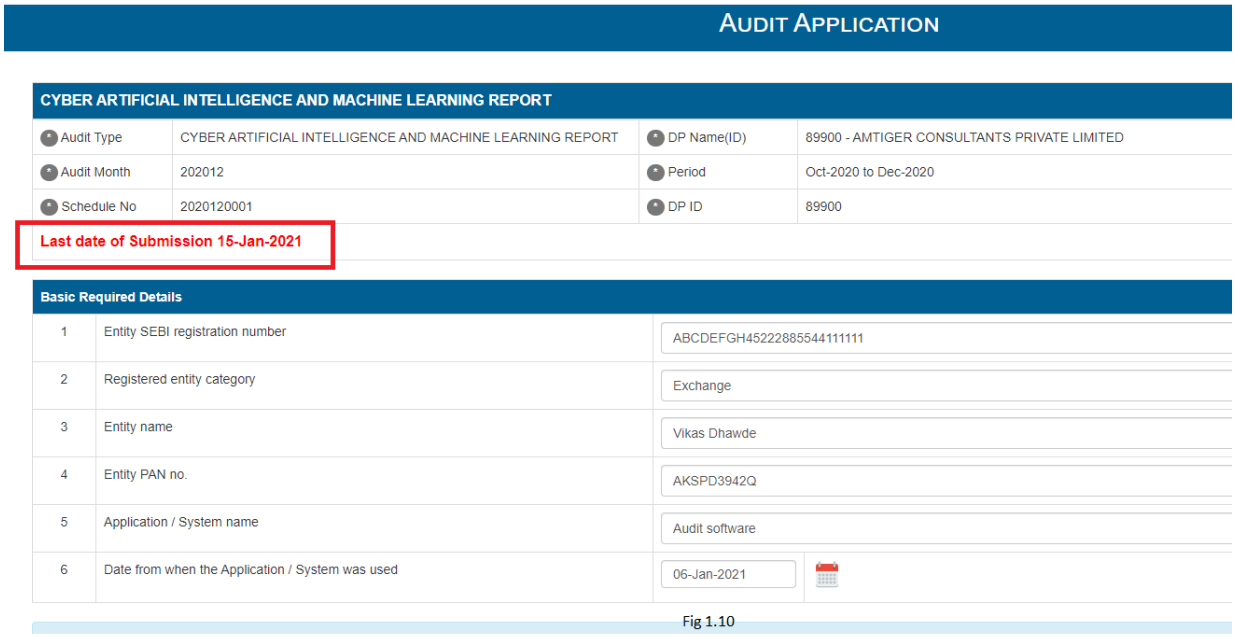


Fig 1.10

FOR SR.NO 7A, 7B, 7C, 7D AND 11. SYSTEM EXCEPT ONLY 'YES/NO/NA'. KINDLY REFER INSTRUCTION FOR REFERNCE.

Sr no.	Head	Instruction	Values
7	Type of area where AI or ML is used	order execution / Advisory services / KYC / AML / Surveillance / compliance/others (please specify in 256 characters)	ffhhhhhhhhhhhhhhhhhhhhhhhhhhhheeeeeeeeeeeeeeeeeeeeeeeeeeeeevvvvvvvvvvvvvvvvvvvvvvvvvvvvvwwwwwwwwwwwwwwwwwwwwwwwwwtttttttttttttttttttttttttttttttttttt uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuttttttttttttttttttttttttttt
7a	Does the system involve order initiation, routing and execution?	Yes / NO	Yes
7b	Does the system fall under discretionary investment or Portfolio management activities?	Yes / NO	No
7c	Does the system disseminate investment or trading advice or strategies?	Yes / NO	No
7d	Is the application/system used in area of Cyber Security to detect attacks?	Yes / NO	yes
7e	What claims have been made regarding AI and ML Application / System – if any?	free text field	sdfsdfdfdssddggdflmlk
8	What is the name of the Tool / Technology that is categorized as AI and ML system / Application and submissions are declared vide this response	free text field	dvdfgmfvkmdfklgfklvmf'
9	How was the AI or ML project implemented	Internally / through solution provider / Jointly with a solution provider or third party	fbgkkertregnkfkvmm,f
10	Are the key controls and control points in your AI or ML application or systems in accordance to circular of SEBI that mandate cyber security control requirements	free text field	dfgdfgnoolujhg rht grr g e
11	Is the AI / ML system included in the system audit, if applicable?	NA / Yes / NO	Yes
12	Describe the application / system and how it uses AI / ML as portrayed in the product offering	free text field	gfhmgrmvbkmg
13	What safeguards are in place to prevent abnormal behavior of the AI or ML application / System	free text field	dfgfg

Save | Submit | View, Save File and Attach Digital Signature | Upload AIML File | Attach Files

Fig 1.11

AI & ML report status

DP IT Official / CISA Auditor Details

Delete	User Type	Mobile No.	Email ID
Delete	DP IT Official	9967139008	vikasd@cdslindia.com
Delete	DP IT Official	1335544228	saritay@cdslindia.com
Delete	DP IT Official	7777777777	hemantm@cdslindia.com
Delete	DP IT Official	5555555555	sameerm@cdslindia.com
Delete	CISA Auditor	9999999999	vikasd@cdslindia.com

REPORT STATUS

Status	View Report / View File
Audit Type	CYBER ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING REPORT
Fetch Details	

Fig 1.12

Quarterly Cyber Incident report

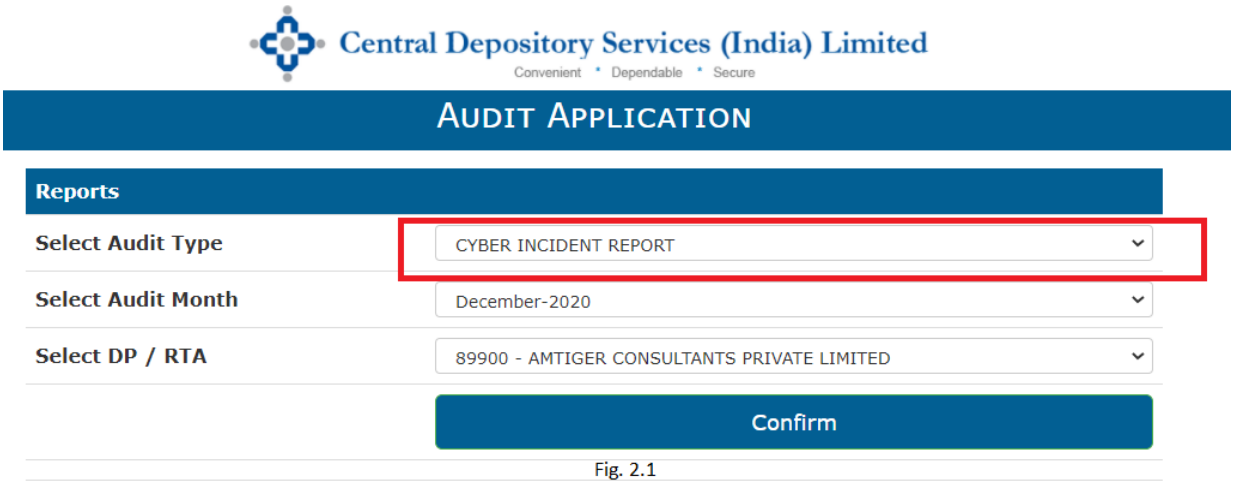


Fig. 2.1

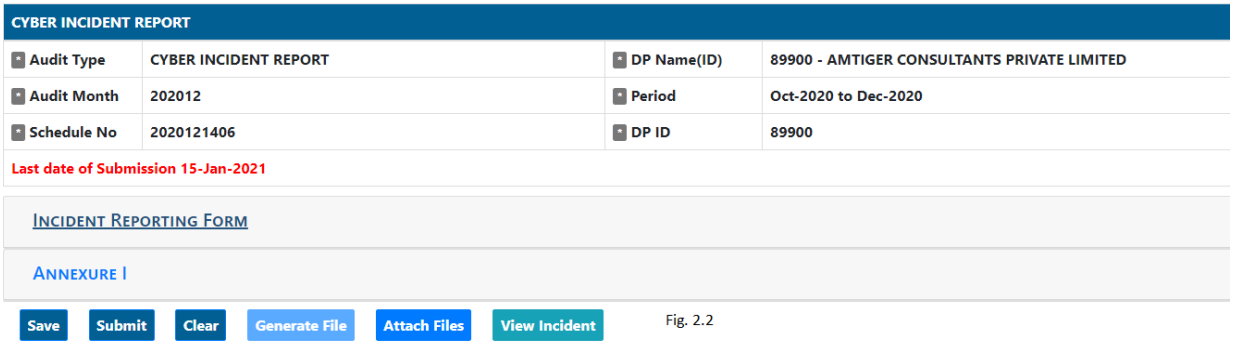


Fig. 2.2

DP IT Official can save multiple incident report which occurr during the respective quarter.

- Whenever DP saves the record new incident ID will populate in system.
- Once DP IT official click on “Submit” button then DP will not able to save / modify the record.
- DP can upload supporting documents into the system.
- After generating Incident report, DP needs to attach digital signature in the report and upload in system. Once digitally signed report uploaded in system, system will automatically close the report.

Last date of Submission 15-Jan-2021

INCIDENT REPORTING FORM

Incident Reporting Form

1. Letter/Report Subject

NAME OF THE DEPOSITORY PARTICIPANT	89900 - AMTIGER CONSULTANTS PRIVATE LIMITED	UNIQUE INCIDENT NO. :- 2	
NAME OF DEPOSITORY	CDSL	Financial Year = 2020-2021	
MEMBER ID / DP ID	89900		

2. Reporting Periodicity Year

QUARTER 3 [OCT-2020 TO DEC-2020]

3. Designated Officer (Reporting Officer details)

* NAME	Name	* ORGANIZATION	Organization name
TITLE	Title	* EMAIL ID	Email ID
PHONE / FAX NO.	Phone / Fax No	* MOBILE	Mobile
ADDRESS	Address		

Fig. 2.3

ANNEXURE I

Annexure I

1. Physical location of affected computer / Network and name of ISP

Physical location of affected computer / Network and name of ISP

2. Date and time incident occured

dd-MMM-yyyy *

3. Information of affected system

IP ADDRESS	IP Address	COMPUTER / HOST NAME	
LAST PATCHED / UPDATED	dd-MMM-yyyy	OPERATING SYSTEM (INCL. VER / RELEASE NO.)	
HARDWARE VENDOR / MODEL	Hardware model		

4. Type of incident

☐ PHISHING	☐ WEBSITE DEFACEMENT	☐ BOT/BOTNET	☐ DISTRIBUTED DENIAL OF SERVICE(DDOS)	☐ SOCIAL ENGINEERING
☐ NETWORK SCANNING / PROBING BREAK-IN/ROOT	☐ SYSTEM MISUSE	☐ EMAIL SPOOFING	☐ USER ACCOUNT COMPROMISE	☐ TECHNICAL VULNERA
☐ VIRUS/MALICIOUS CODE	☐ SPAM	☐ DENIAL OF SERVICE(DOS)	☐ WEBSITE INTRUSION	☐ IP SPOOFING

5. Description of Incident

Fig. 2.4