National Stock Exchange of India Limited

Circular

DEPARTMENT: INSPECTION	
Download Ref No: NSE/INSP/52249	**Date: May 10, 2022**
Circular Ref. No: 33/2022	

To All Members,

Sub: Cyber Security & Cyber Resilience Audit of Trading Members

Member's attention is drawn to SEBI circular no. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018, SEBI/HO/MIRSD/DOP/CIR/P/2019/109 dated October 15, 2019 and Exchange circular no. NSE/INSP/41723 dated July 26, 2019 in relation to Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants.

Reference is further drawn to the para 5 of the said SEBI Circular dated October 15, 2019 wherein periodicity of audit for the purpose of compliance with Cyber Security and Cyber Resilience is defined. Accordingly, trading members are required to carry-out audit for the period ended March 31, 2022, as per the applicability criteria given below.

Category of Member	Type I	Type II Using NNF	Type III Using Algo
Trading Members	Annually	Annually	Half Yearly

The link for the submission of Cyber Security & Cyber Resilience Audit report is activated. The procedure for submitting thereport by member and auditor through ENIT module in the Member portal is provided in Annexure- A and Annexure- B respectively. Timelines for submissions of Audit report is given below:

Audit Period	Due date for submission		
	Preliminary Audit Report submission	**Action Taken Report (ATR) Submission (if applicable)**	**Follow-on Audit Report Submission (if applicable)**
Half Yearly (October 2021-March 2022)	June 30, 2022	September 30, 2022	December 31, 2022
Annual Submission (April 2021- March 2022)	June 30, 2022	September 30, 2022	December 31, 2022

Submission of Cyber Security & Cyber Resilience Audit Report shall be considered completed only after trading member submits the report to the Exchange after providing management comments.

The following penalty/disciplinary actions would be initiated against the Member for late/non-submission of Cyber Security & Cyber Resilience Security Audit Report.

Particulars	**Action**
Submission within 1 month from the end of due date of submission.	Penalty of Rs. 200/- per day
Submission after 1 month but within 3 months from the end of the due date for submission.	Penalty of Rs. 500/- per day
Non-Submission within 3 months from the end of due date for submission	Disablement of trading facility across segments after giving 2 weeks' notice. Member will be enabled only after submission of Cyber Security & Cyber Resilience audit report.

All Members are advised to take note of the above and comply.

For and on behalf of
National Stock Exchange of India Limited

Swati Sopare
Senior Manager-Inspection

Enclosure:

Annexure A – User guide for Member to submit Cyber Security & Cyber Resilience Audit Report

Annexure B – User guide for Auditor report submission

Annexure C – Auditor Selection Norms

Annexure D – Terms of Reference (TOR) for Cyber Security & Cyber Resilience Audit Report

In case of any clarifications, Members may contact our below offices:

Regional Office	**E MAIL ID**	**CONTACT NO.**
Ahmedabad (ARO)	inspectionahm@nse.co.in	079- 49008632
Chennai (CRO)	inspection_cro@nse.co.in	044- 66309915 / 17
Delhi (DRO)	delhi_inspection@nse.co.in	011- 23459127 / 38 / 46
Kolkata (KRO)	inspection_kolkata@nse.co.in	033- 40400411 / 405
Mumbai (WRO)	compliance_wro@nse.co.in	Board Line: 022-25045000 / 022-61928200 Direct Line: 022-25045138 / 022-25045144 Extn: 28144 / 28138
Central Help Desk	compliance_assistance@nse.co.in	

Annexure A

User guide to submit Cyber Security & Cyber Resilience Audit for Member

A) Registration of Auditor

1) Admin User need to create 2 user ids in Member Portal.

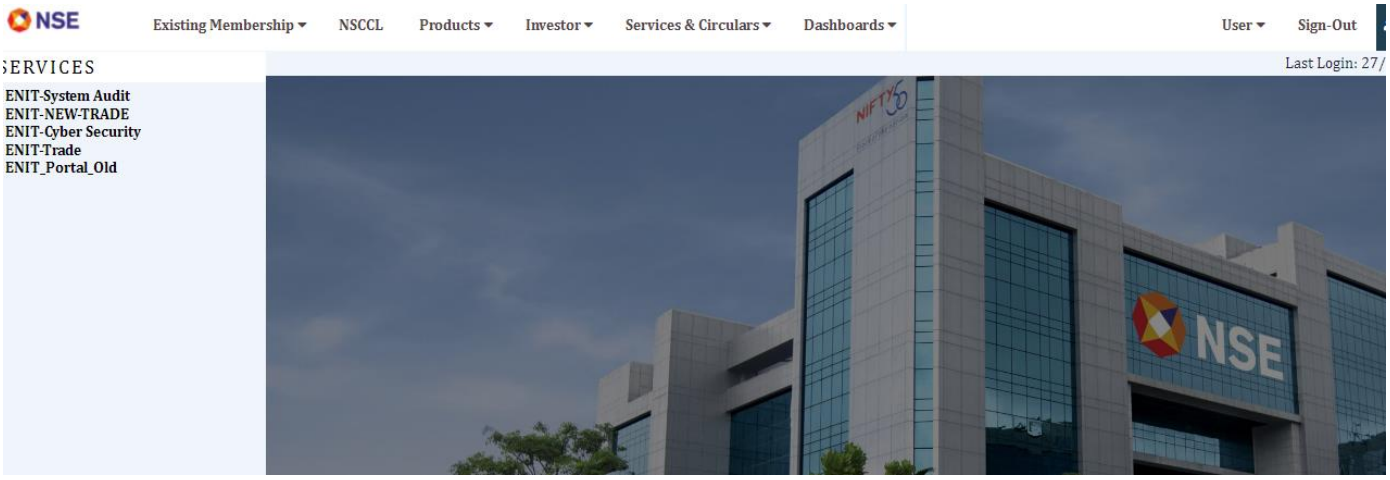
   a) One user id for the user at member's end who will register Auditor and submit the final Audit Report from member's end. Here Admin will assign '**ENIT- NEW-TRADE'** role to user.

Services:	ALL	CD	CM	CO	DEBT	FO	MFSS	REPO	SLB	WDM
ENIT-Affiliates	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
ENIT-COMPLIANCE-NEW	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
ENIT-Compliance	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
ENIT-Compliance-NEW1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
ENIT-Compliance-NEW2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
ENIT-Cyber Security	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
ENIT-INV-ASSETS-AUDITOR	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
ENIT-NEW-Service-Request	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
ENIT-NEW-TRADE	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐
ENIT-Service Request	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
ENIT-System Audit	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
ENIT-Trade	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
ENITHalfYearly	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

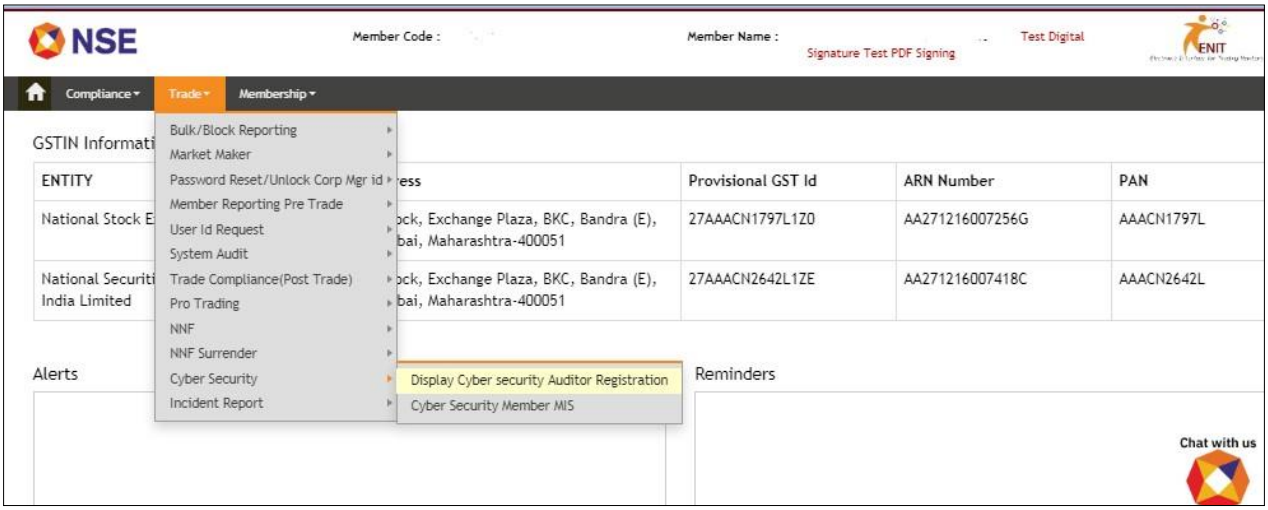
   b) Then second user id is to be created for Auditor. Here Admin will assign '**ENIT-Cyber Security'** role to Auditor

Services:	ALL	CD	CM	CO	DEBT	FO	MFSS	REPO	SLB	WDM
ENIT-Affiliates	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
ENIT-COMPLIANCE-NEW	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
ENIT-Compliance	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
ENIT-Compliance-NEW1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
ENIT-Compliance-NEW2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
ENIT-Cyber Security	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐
ENIT-INV-ASSETS-AUDITOR	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
ENIT-NEW-Service-Request	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
ENIT-NEW-TRADE	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
ENIT-Service Request	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
ENIT-System Audit	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
ENIT-Trade	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
ENITHalfYearly	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

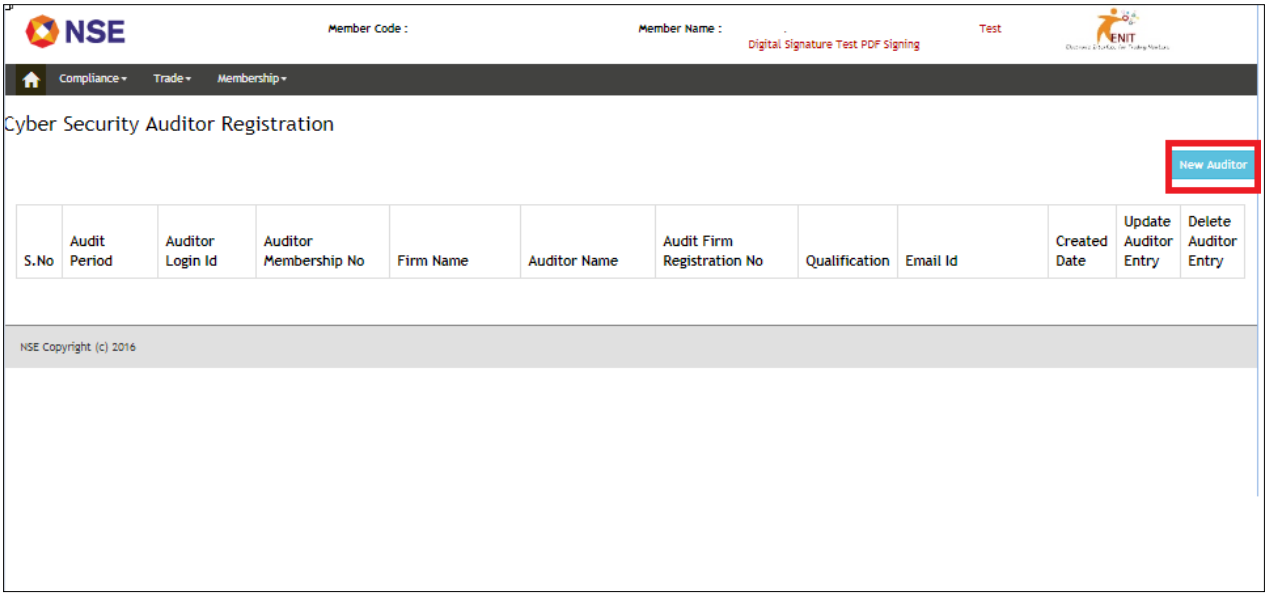
2) Member User having ENIT-NEW TRADE, will now have to register Auditor in ENIT. User will get below screen after login. User need to click on ENIT-NEW-TRADE.



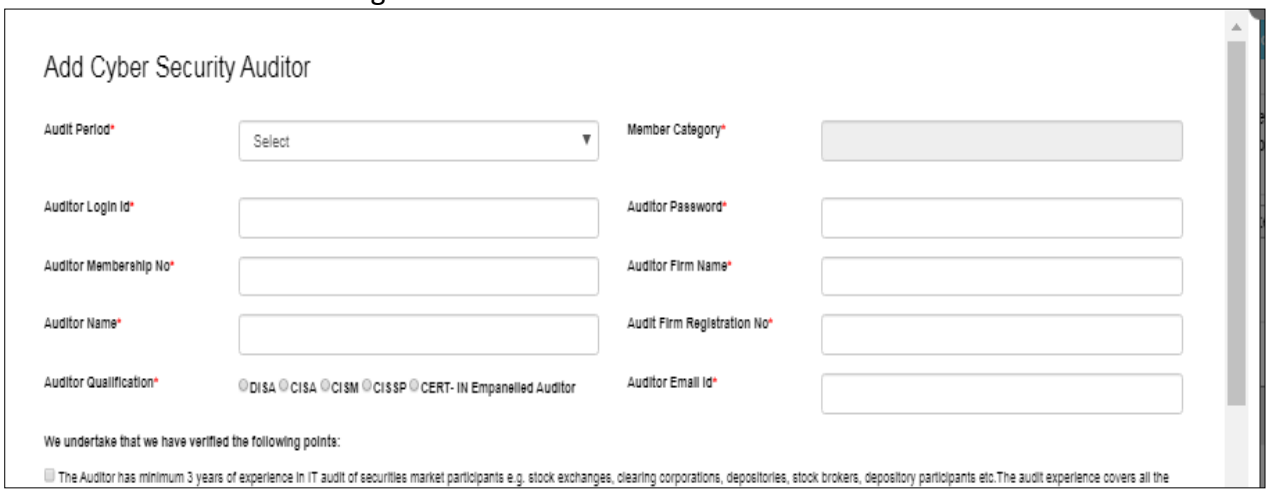
3) After clicking on ENIT-NEW-TRADE, user will get below screen. Click on **Trade > Cyber Security > Display Cyber Security Auditor Registration**



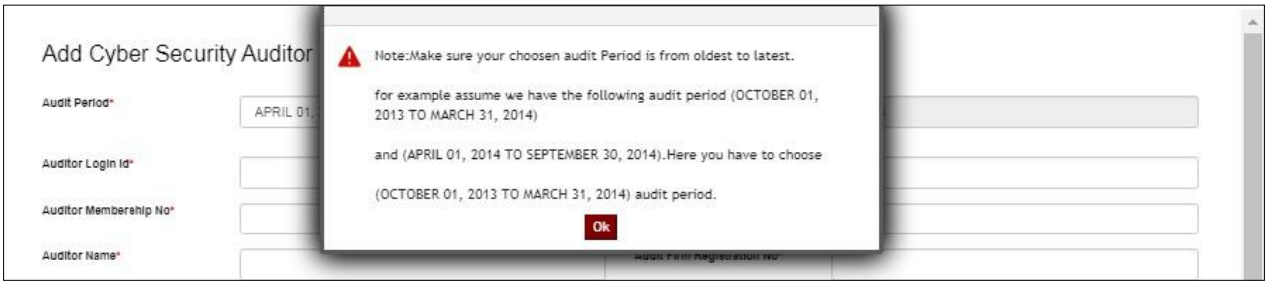
4) Click on New Auditor for registering Auditor for the current period.



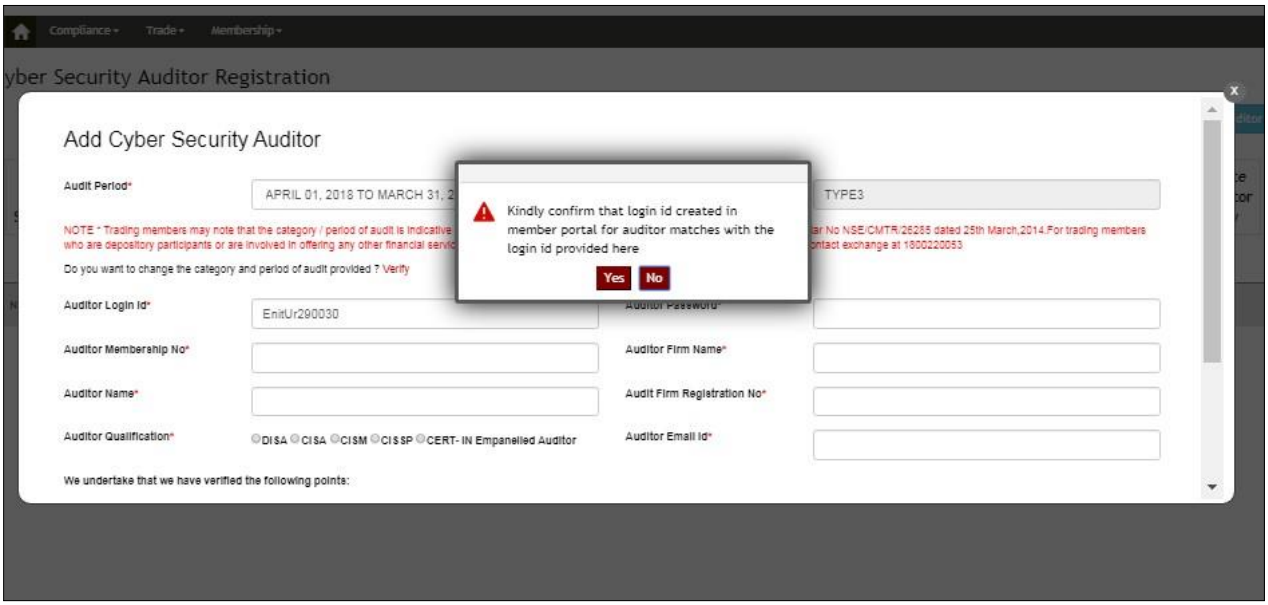
5) Fill the details for Auditor Registration.



6) On selecting Audit Period User will get below screen. Ensure that you are registering Auditor for the oldest period and Click on 'Ok' button.

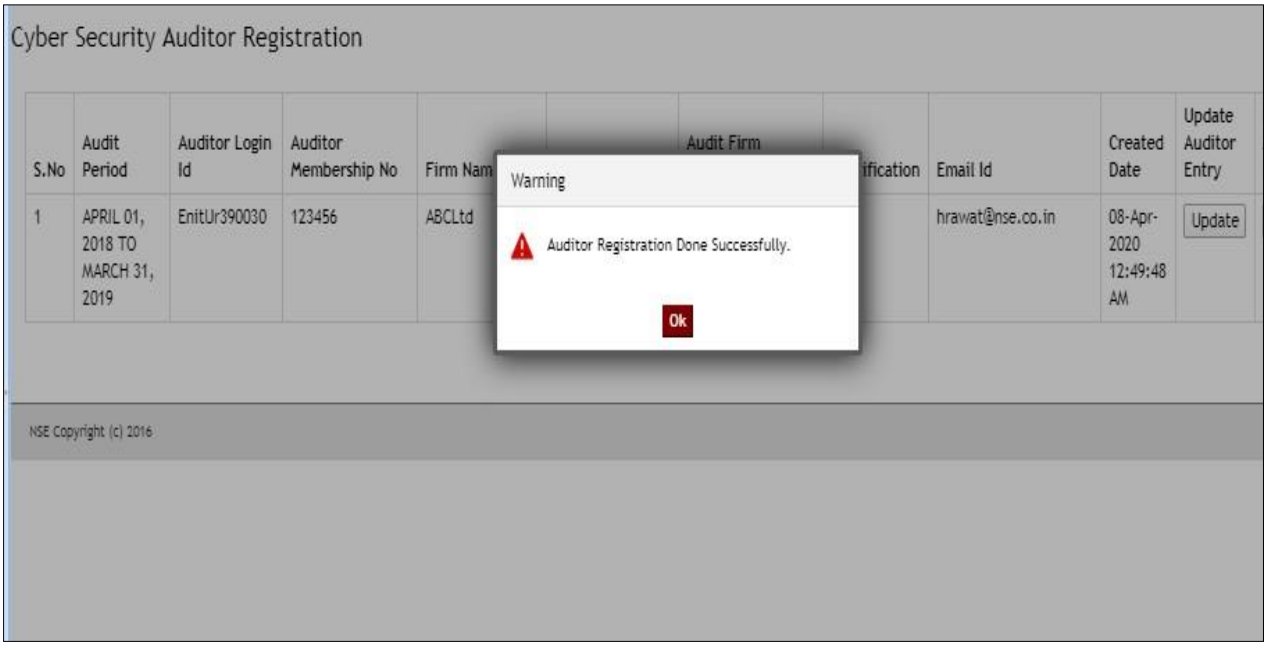


7) While Entering Login details, it is to be noted that the Auditor Login details should be same as that in Member Portal.



8) After entering all details click on Submit. On submitting you will get below pop-up, click on 'Ok'

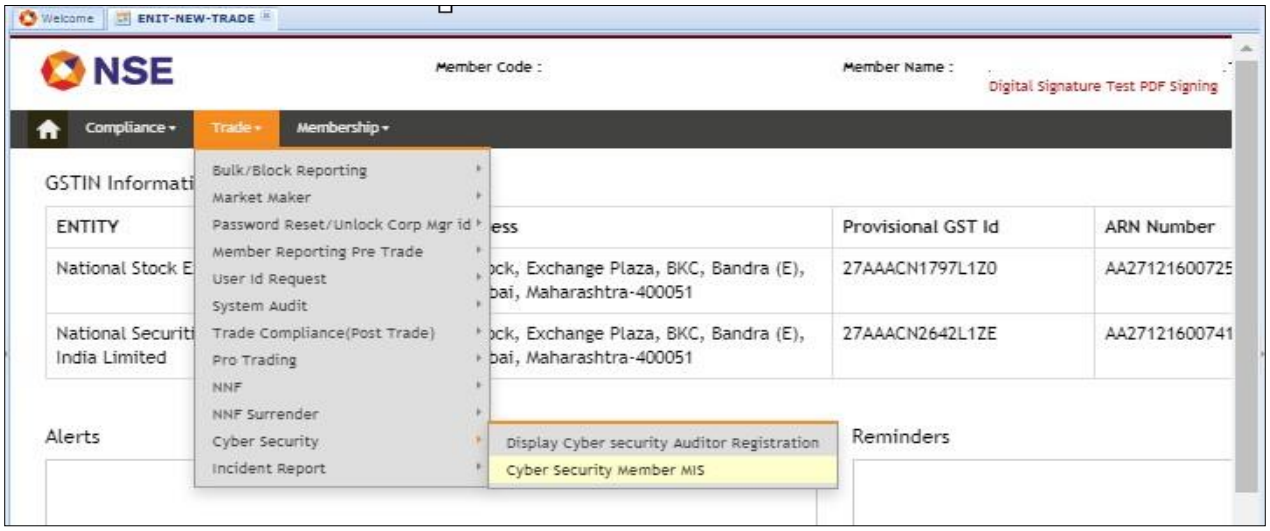
9) On clicking 'Ok' user will get below message of successful Auditor registration.



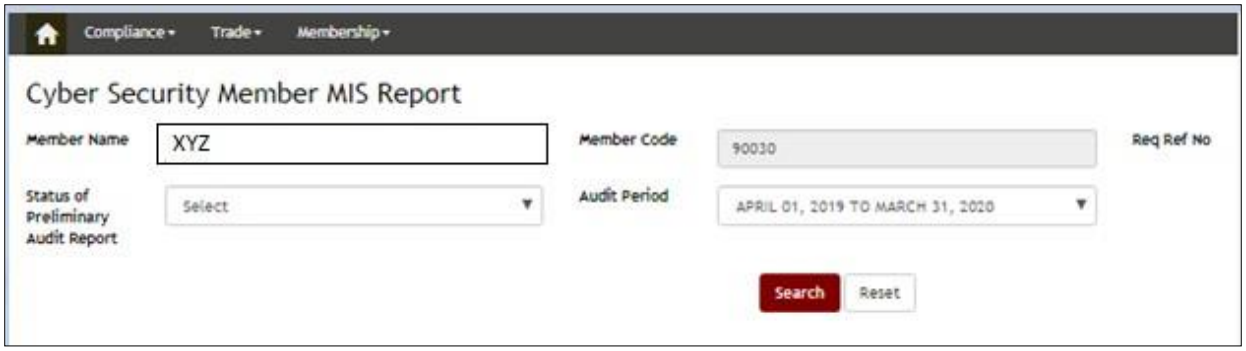
Auditor Registration completed here. Auditor will submit the report. Once Auditor submits the report below procedure to be followed.

B) Submission of Audit Report by Member

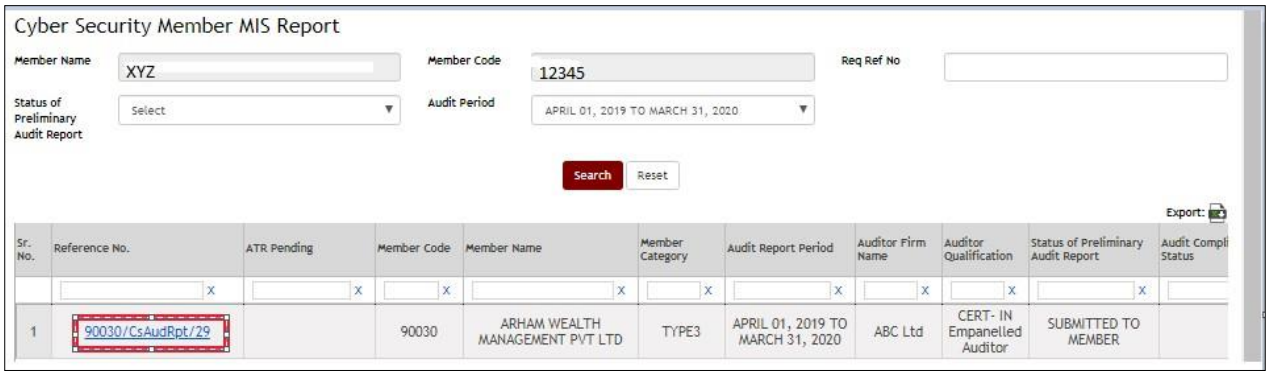
1) Once Auditor submits the report in system, Member have to login in system. Click on ENIT –NEW-TRADE> Trade > Cyber Security >Cyber Security Member MIS.



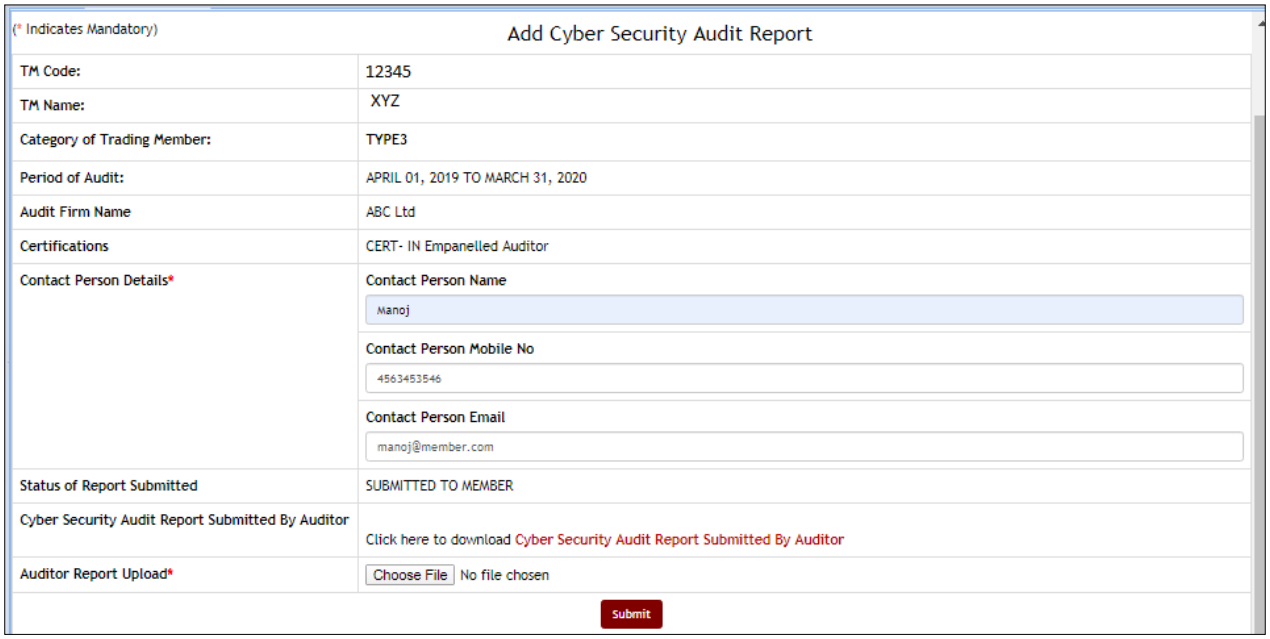
2) Select period and click on Search button



3) Click on Reference No. link

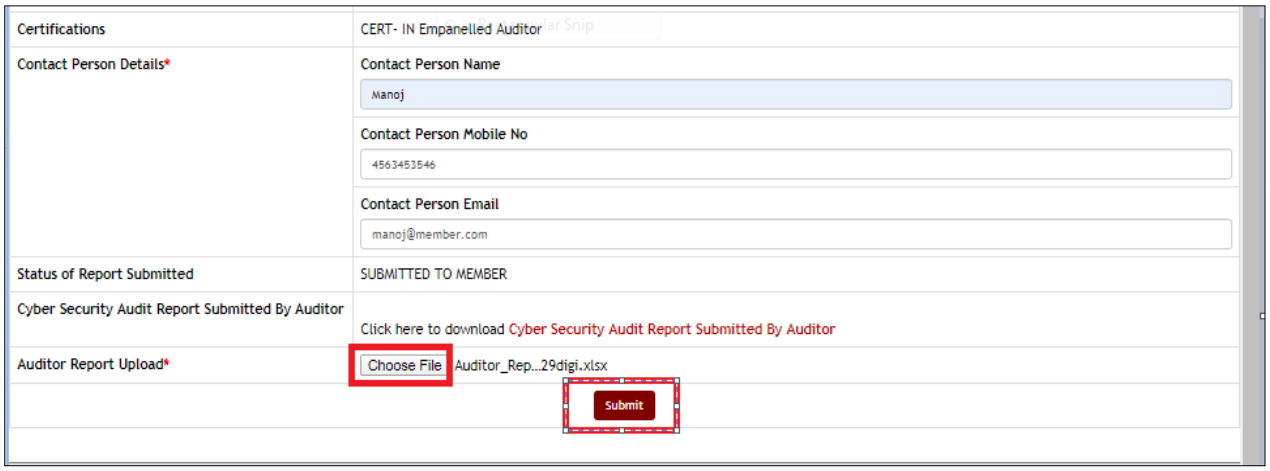


4) Fill require Contact Person Details, download Audit report from the link given in red font.

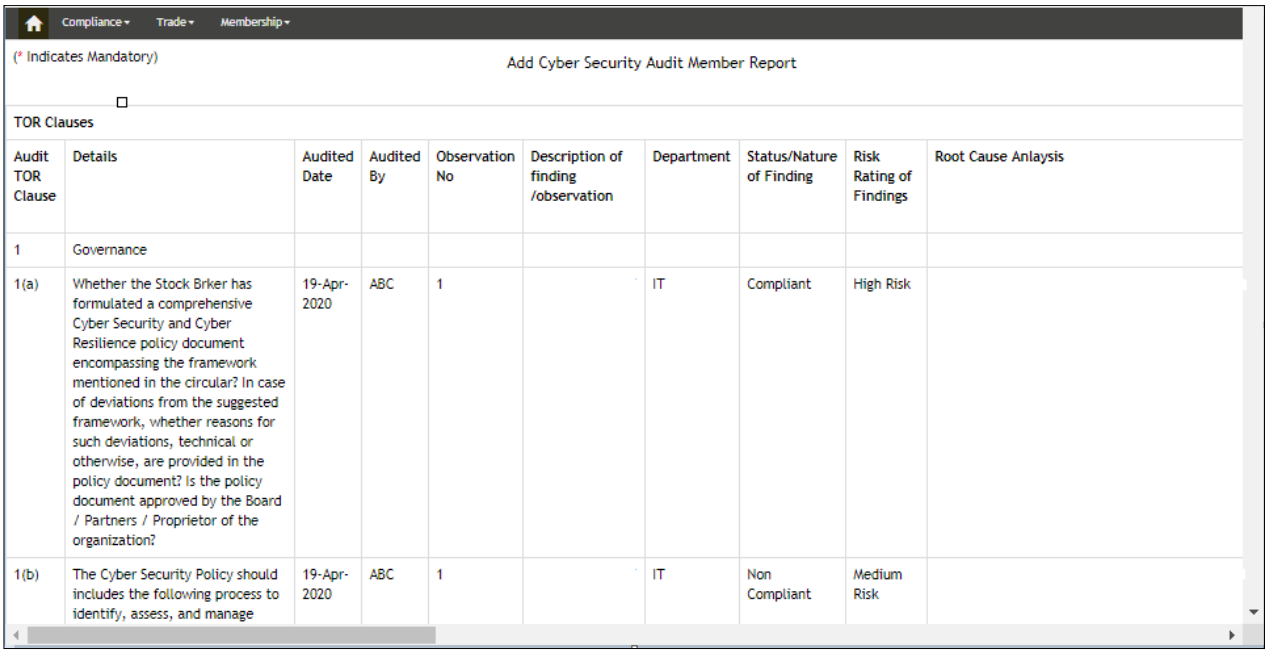


Update Trading Member Management Comments in the excel report.

5) Browse and upload the report having management comments and then click on submit.

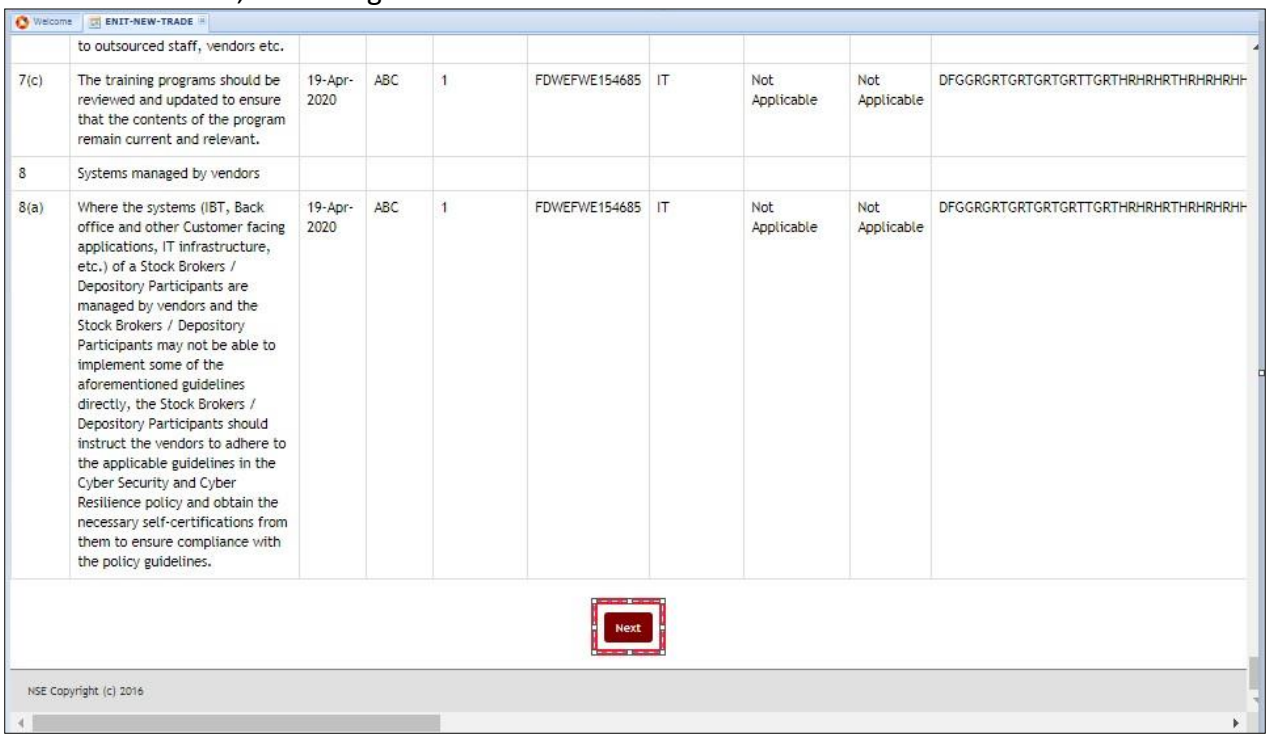


6) User will see the preview of report on screen. User can check error if any in Error Description column which is the last column in this preview screen. If there is any error given, click on 'Back' button in the middle bottom of the screen and upload the report again after doing necessary changes.



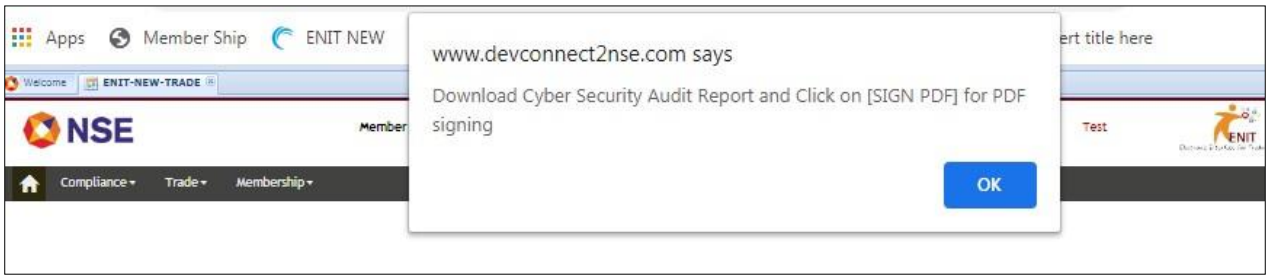
Audit TOR Clause	Details	Audited Date	Audited By	Observation No	Description of finding /observation	Department	Status/Nature of Finding	Risk Rating of Findings	Root Cause Anlaysis
1	Governance								
1(a)	Whether the Stock Brker has formulated a comprehensive Cyber Security and Cyber Resilience policy document encompassing the framework mentioned in the circular? In case of deviations from the suggested framework, whether reasons for such deviations, technical or otherwise, are provided in the policy document? Is the policy document approved by the Board / Partners / Proprietor of the organization?	19-Apr-2020	ABC	1		IT	Compliant	High Risk	
1(b)	The Cyber Security Policy should includes the following process to identify, assess, and manage	19-Apr-2020	ABC	1		IT	Non Compliant	Medium Risk	

7) If there is no error, user will get 'Next' button at the bottom of the screen. Click on the 'Next' button.



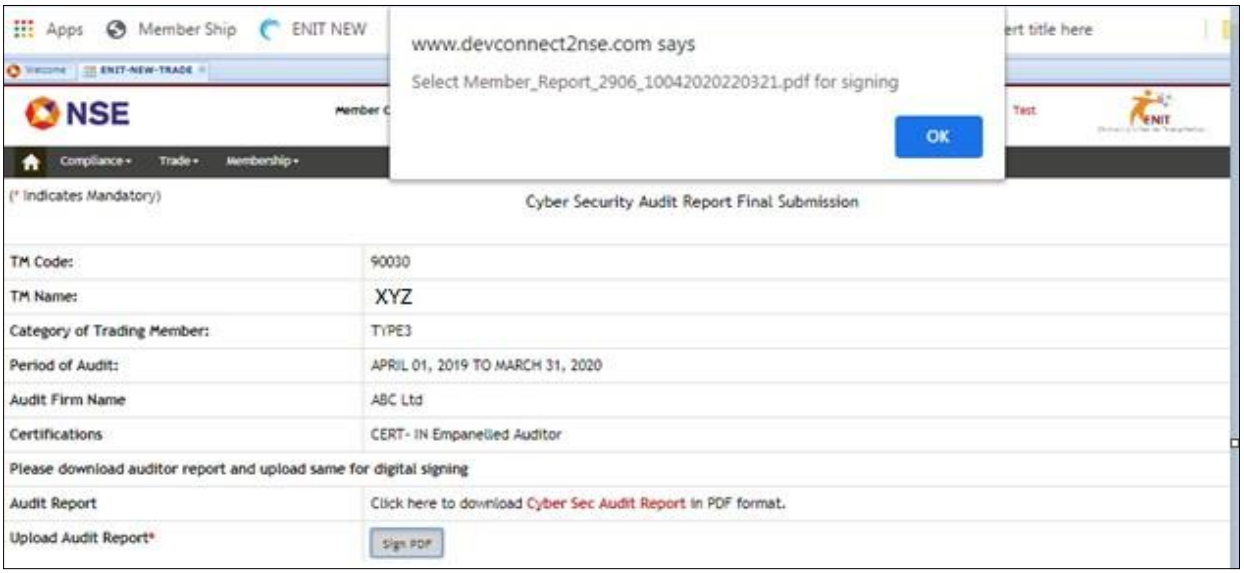
	to outsourced staff, vendors etc.								
7(c)	The training programs should be reviewed and updated to ensure that the contents of the program remain current and relevant.	19-Apr-2020	ABC	1	FDWEFWE154685	IT	Not Applicable	Not Applicable	DFGGRGRTGRTGRTGRTTGRTHRHRHRTHRHRHRHH
8	Systems managed by vendors								
8(a)	Where the systems (IBT, Back office and other Customer facing applications, IT infrastructure, etc.) of a Stock Brokers / Depository Participants are managed by vendors and the Stock Brokers / Depository Participants may not be able to implement some of the aforementioned guidelines directly, the Stock Brokers / Depository Participants should instruct the vendors to adhere to the applicable guidelines in the Cyber Security and Cyber Resilience policy and obtain the necessary self-certifications from them to ensure compliance with the policy guidelines.	19-Apr-2020	ABC	1	FDWEFWE154685	IT	Not Applicable	Not Applicable	DFGGRGRTGRTGRTGRTTGRTHRHRHRTHRHRHRHH

8) Click ‘Ok’ on pop-up message

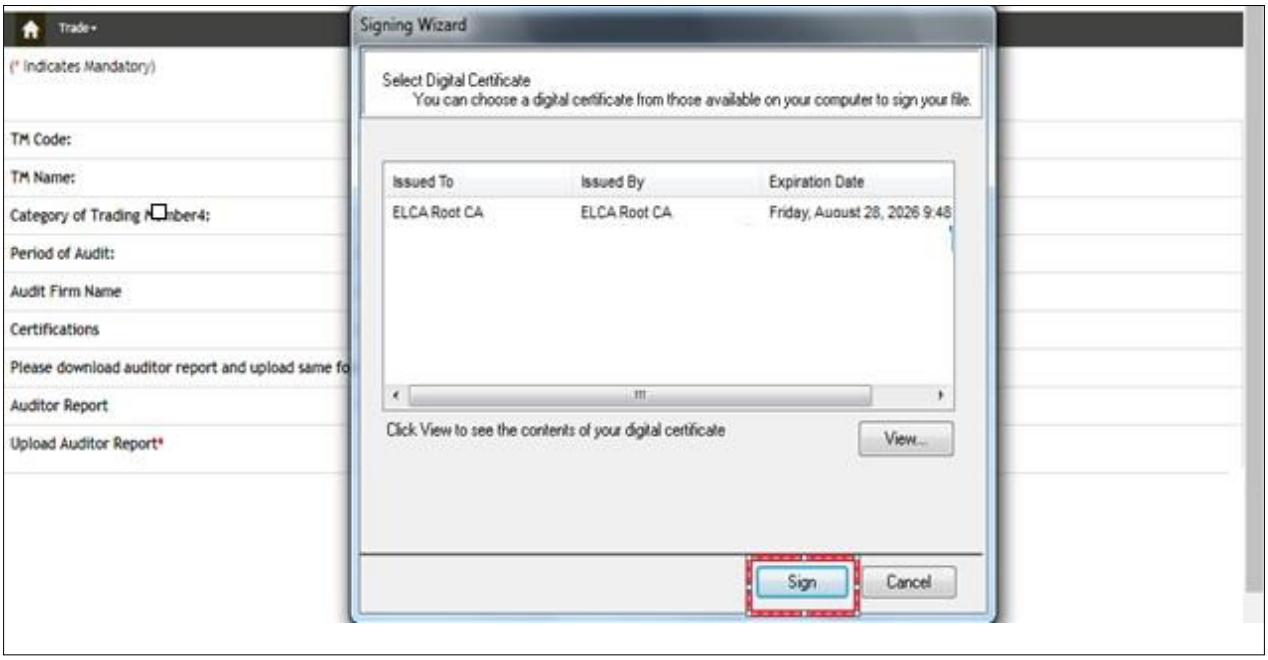


9) Download the PDF report by clicking on ‘Cyber Sec Audit Report’ link. Click on ‘Sign PDF’

10) On clicking Sign PDF, user will get pop-up as shown in below screen, click on ‘Ok’. Then user will be able to browse the report. Select the same PDF report which is downloaded without renaming.

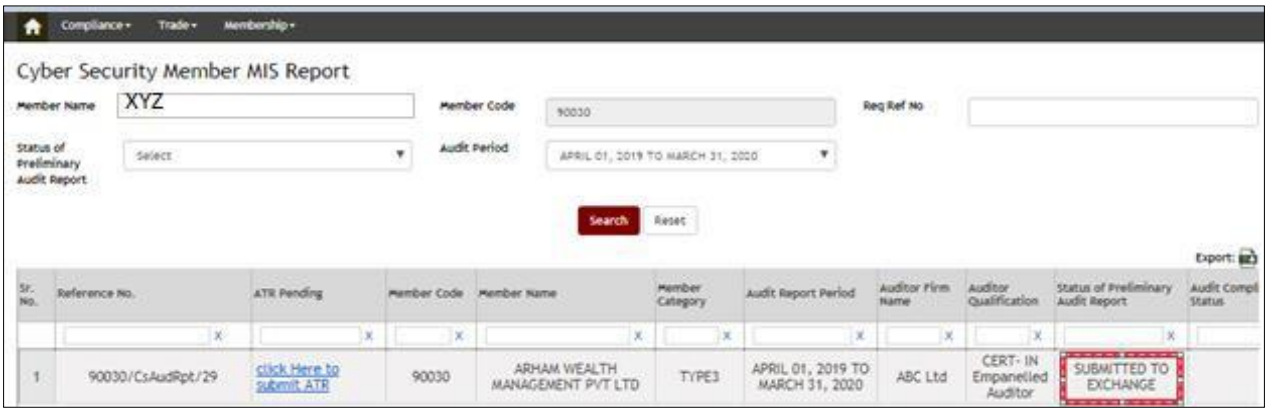

Apps
Member Ship
ENIT NEW
www.devconnect2nse.com says
Select Member_Report_2906_10042020220321.pdf for signing
OK
NSE
Compliance
Trade
Membership
(* Indicates Mandatory)
Cyber Security Audit Report Final Submission
TM Code: 90030
TM Name: XYZ
Category of Trading Member: TYPE3
Period of Audit: APRIL 01, 2019 TO MARCH 31, 2020
Audit Firm Name ABC Ltd
Certifications CERT- IN Empanelled Auditor
Please download auditor report and upload same for digital signing
Audit Report Click here to download Cyber Sec Audit Report in PDF format.
Upload Audit Report*
Sign PDF

11) After browsing, user will get a window for selecting Signature. Select the signature and click on 'Sign'

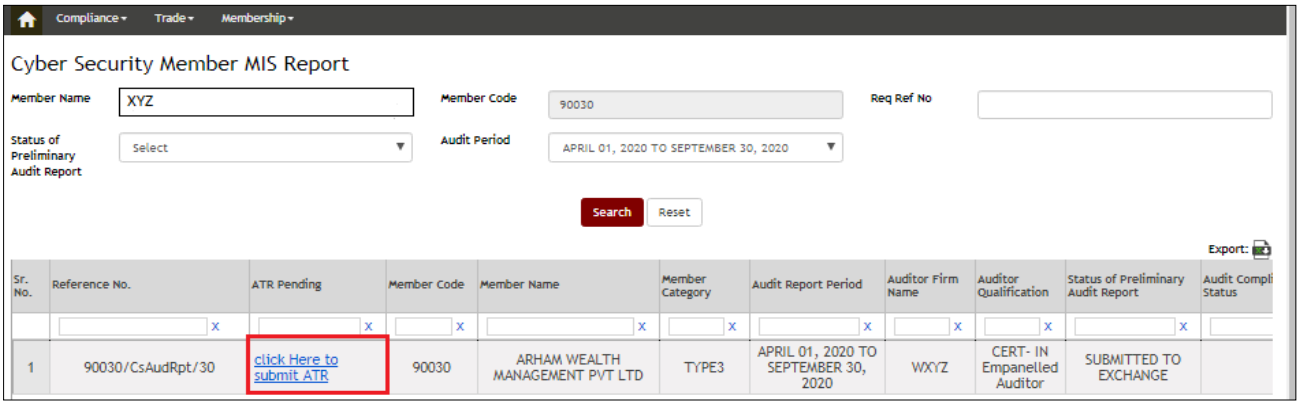


12) Save the signed file in your system and browse the same after clicking on 'Choose File button. Now click on Submit button.

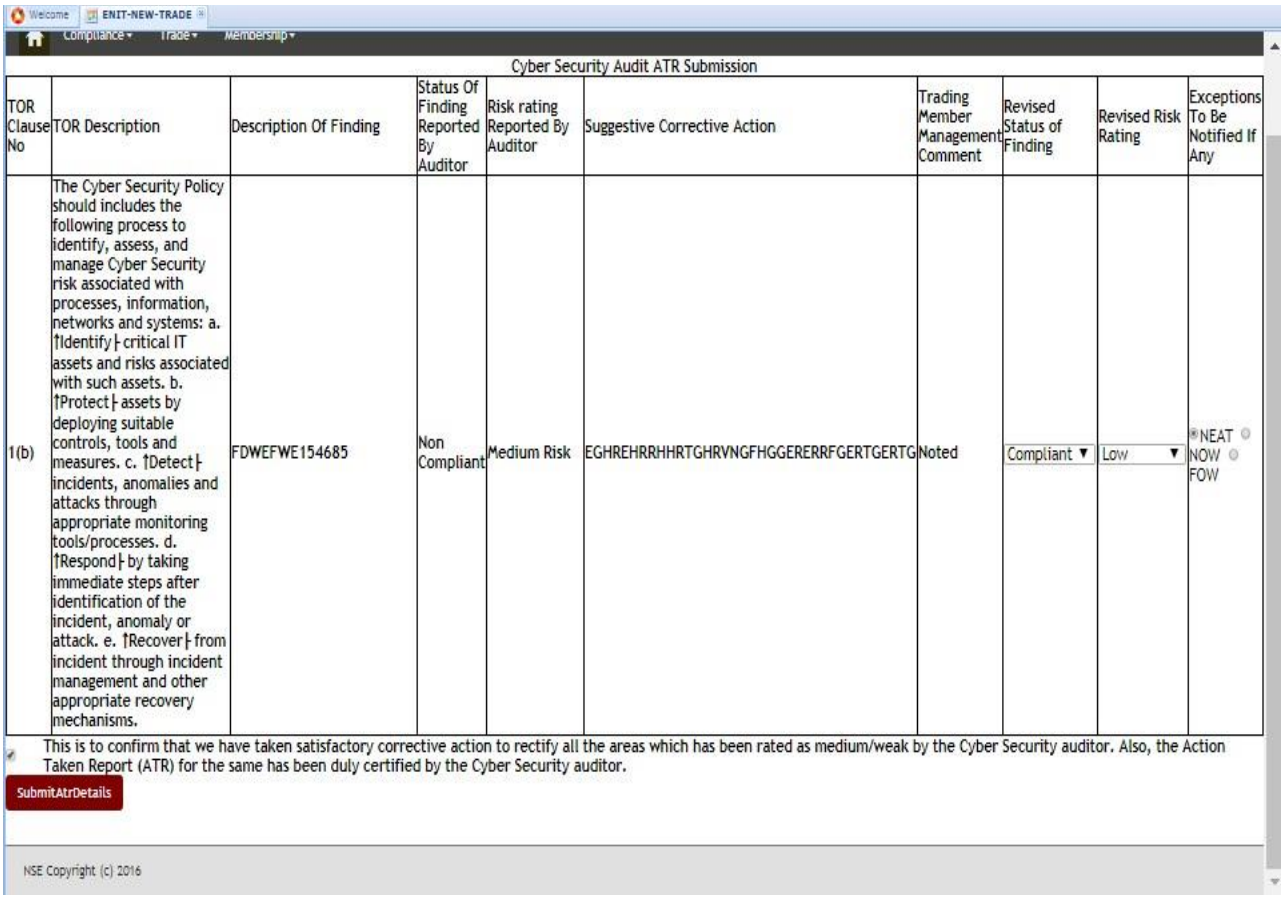
13) Member can check the status in Cyber Security Member MIS Report



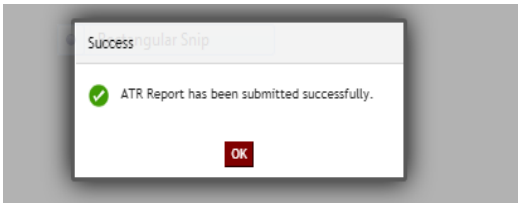
14) Further, if Auditor has given ATR requirement, member need to submit the ATR in system by clicking on the link given in Cyber Security Member MIS Report.



15) Fill the require details > Click on Declaration Checkbox > Submit



Below message after successful submission.



Annexure B

User Manual for Auditor Report Submission

1) Auditor will receive a system generated email once the Auditor Registration is done at Member End. Below is the Email Format. In email, Login id details will be provided Such as Membership No and Identifier No

Dear Sir/Madam,

< Member Name > has registered your firm as Cyber Security Auditor for submission of Cyber security audit report for the period APRIL 01, 2018 TO MARCH 31, 2019

Auditor firm Name: ABC Ltd
Auditor Membership no: 123456
Auditor name: ABC
Audit Firm registration no: 12345678
Kindly click on the following link https://enit.nseindia.com/MemberPortal/home.jsp

Please find the login details as under;
User name: EnitUr290030
Password: Nse@123456
Idntifier: 45869

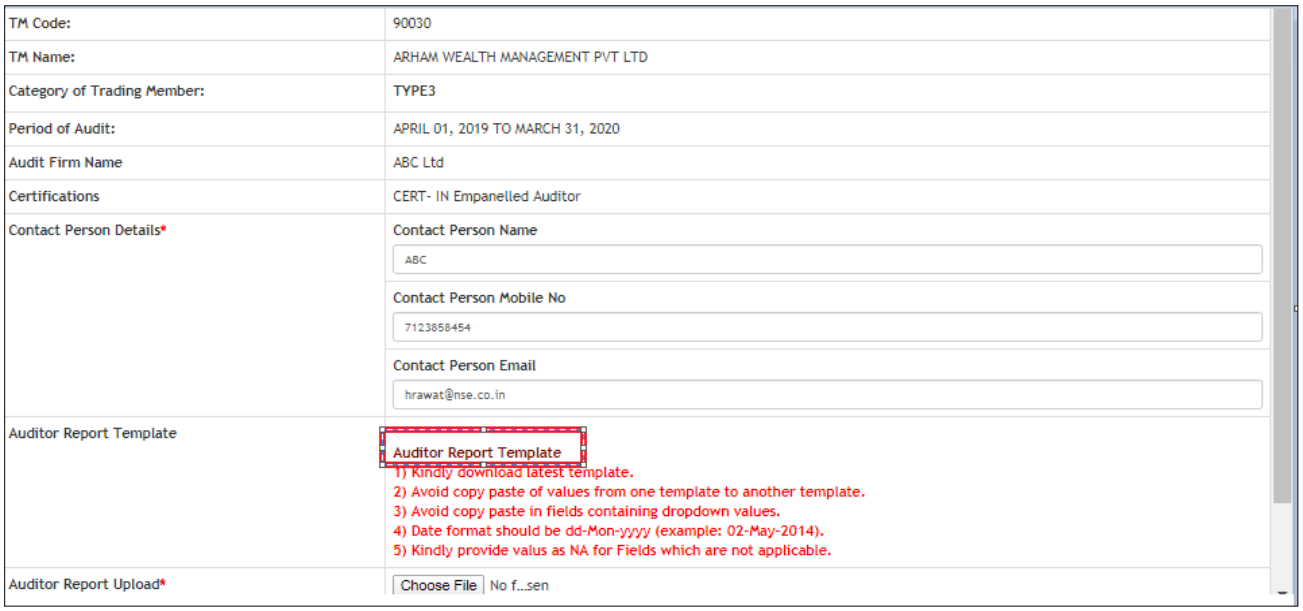
On clicking the above link for the first time, you will be prompted to change the password, Kindly change the password immediately.

2) For Auditor Submission > Login with Auditor login details. Click on ENIT-Cyber Security.

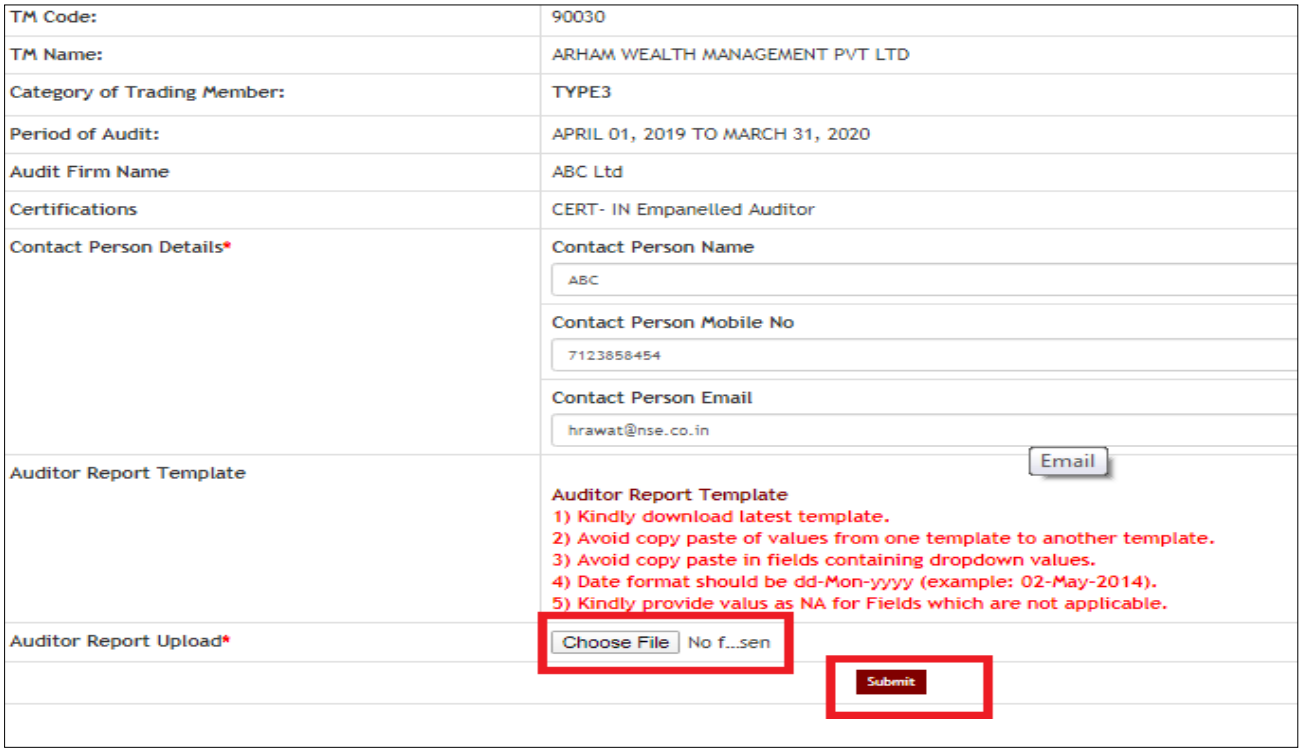
3) Click on Trade > Cyber Security > Cyber Security Auditor MIS.

4) Fill the details and click on Search button. Then click on ‘New Report’ button.

5) On clicking New Report button, below screen will display. Enter the details -> Enter Contact person Name, Contact person No and Contact Person Email. Now click on ‘Auditor Report Template’ link to download the template.

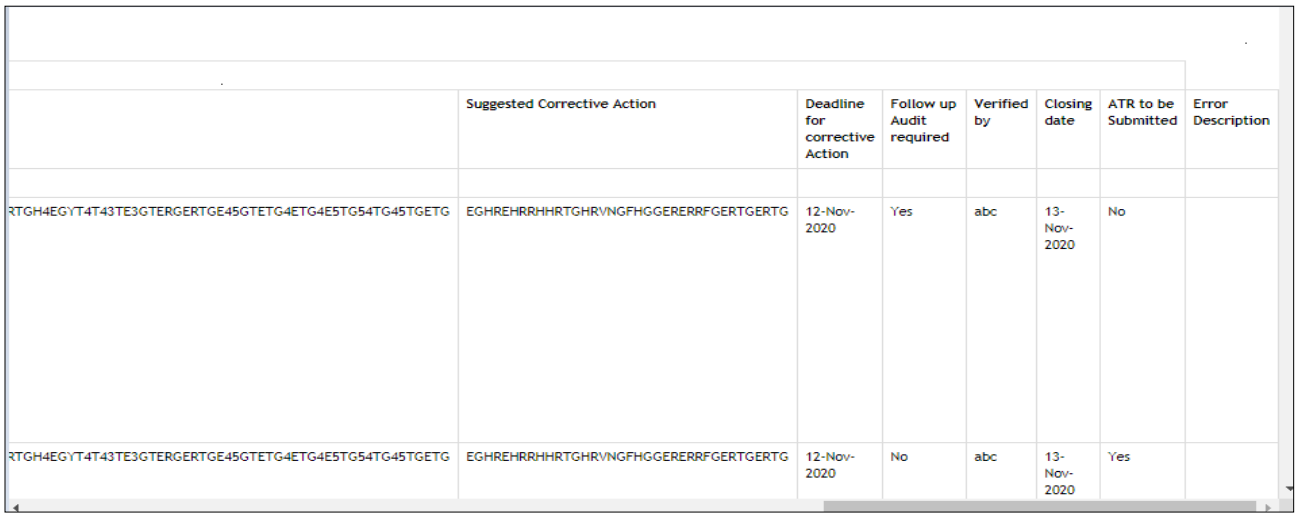


6) After entering required details in template, save the template and upload the file by clicking on 'Choose File' bottom and then click on 'Submit'.



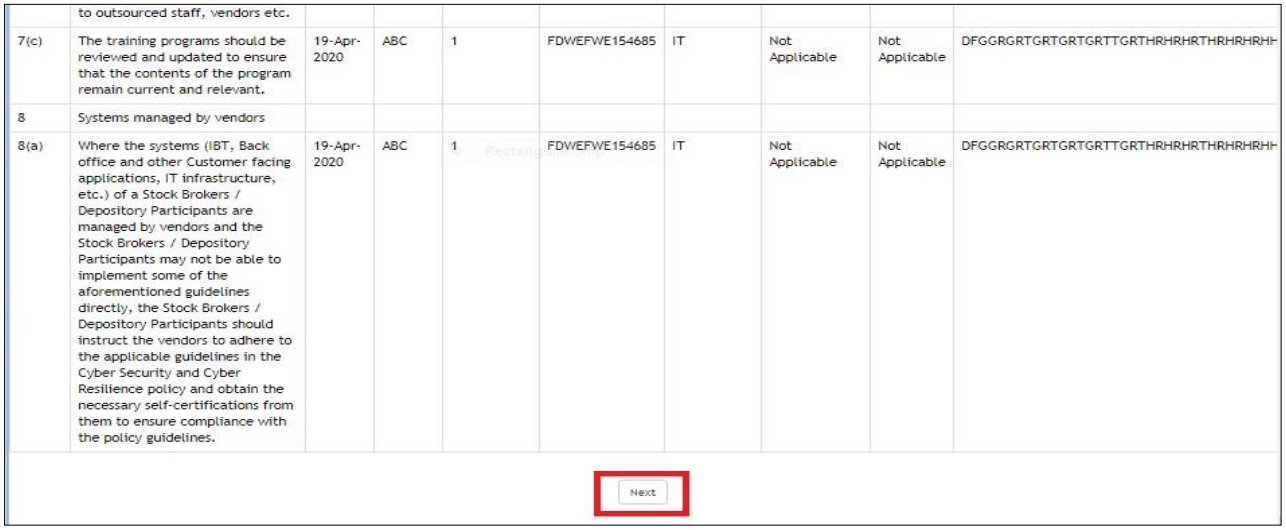
7) After clicking on submit, preview of the report will be shown in the preview screen. Auditor need to verify the same. Error if any found in format will be updated in the 'Error Description' column in preview screen. Auditor need to click 'Back' button at the middle bottom of the screen and upload

the report again after doing needful correction. If there is no error in the format, Auditor will get 'Next' button at the bottom end of the screen.



	Suggested Corrective Action	Deadline for corrective Action	Follow up Audit required	Verified by	Closing date	ATR to be Submitted	Error Description
RTGH4EGYT4T43TE3GTERGERTGE45GTETG4ETG4E5TG54TG45TGETG	EGHREHRRHHRTGHRVNGFHGGERERRFGERTGERTG	12-Nov-2020	Yes	abc	13-Nov-2020	No	
RTGH4EGYT4T43TE3GTERGERTGE45GTETG4ETG4E5TG54TG45TGETG	EGHREHRRHHRTGHRVNGFHGGERERRFGERTGERTG	12-Nov-2020	No	abc	13-Nov-2020	Yes	

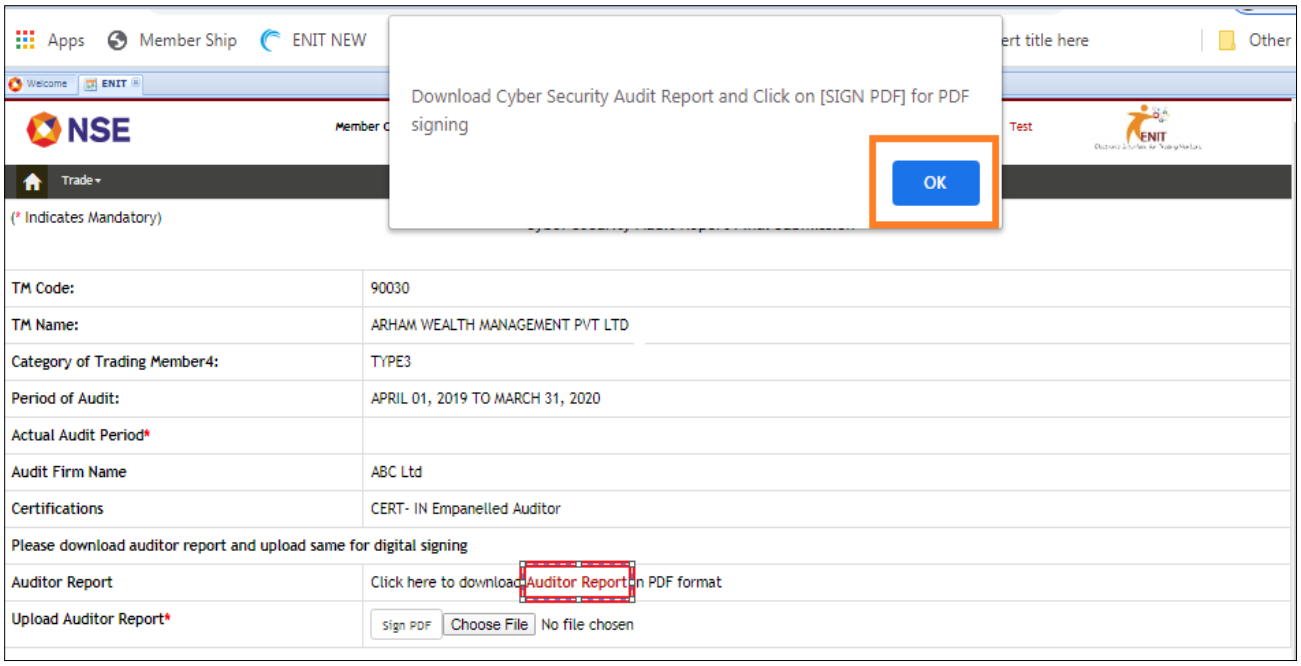
8) Click on next button



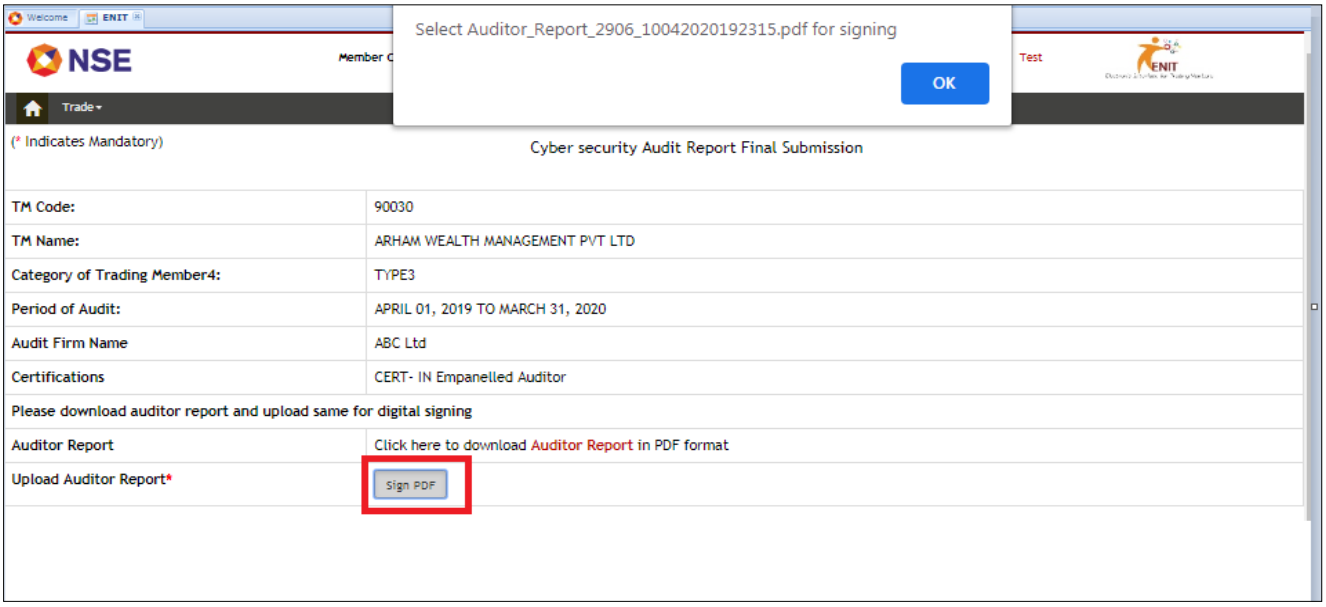
	to outsourced staff, vendors etc.								
7(c)	The training programs should be reviewed and updated to ensure that the contents of the program remain current and relevant.	19-Apr-2020	ABC	1	FDWEFWE154685	IT	Not Applicable	Not Applicable	DFGGRGRTGRTGRTGRTTGRTHRHRHRTHRHRHRHH
8	Systems managed by vendors								
8(a)	Where the systems (IBT, Back office and other Customer facing applications, IT infrastructure, etc.) of a Stock Brokers / Depository Participants are managed by vendors and the Stock Brokers / Depository Participants may not be able to implement some of the aforementioned guidelines directly, the Stock Brokers / Depository Participants should instruct the vendors to adhere to the applicable guidelines in the Cyber Security and Cyber Resilience policy and obtain the necessary self-certifications from them to ensure compliance with the policy guidelines.	19-Apr-2020	ABC	1	FDWEFWE154685	IT	Not Applicable	Not Applicable	DFGGRGRTGRTGRTGRTTGRTHRHRHRTHRHRHRHH

Next

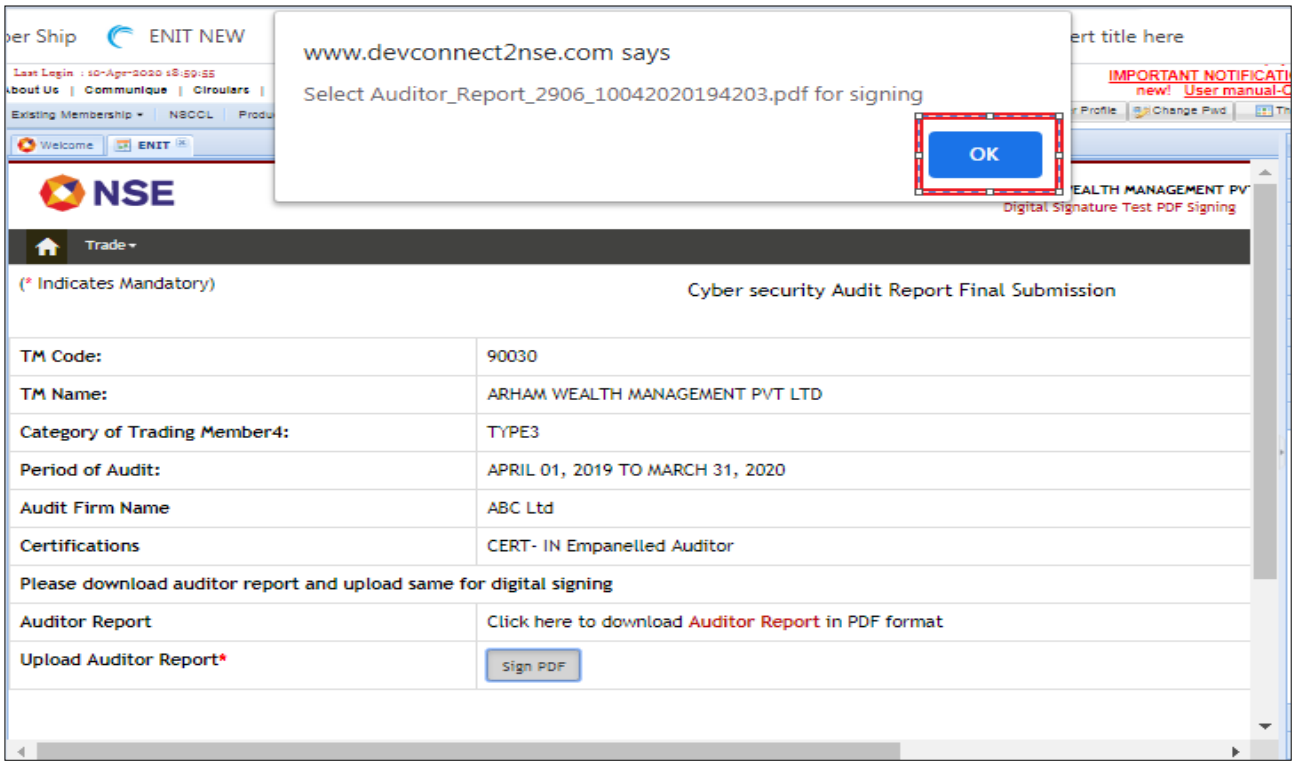
9) Click on 'Ok' for below pop-up and then click on 'Auditor Report' link to download the report in PDF format.



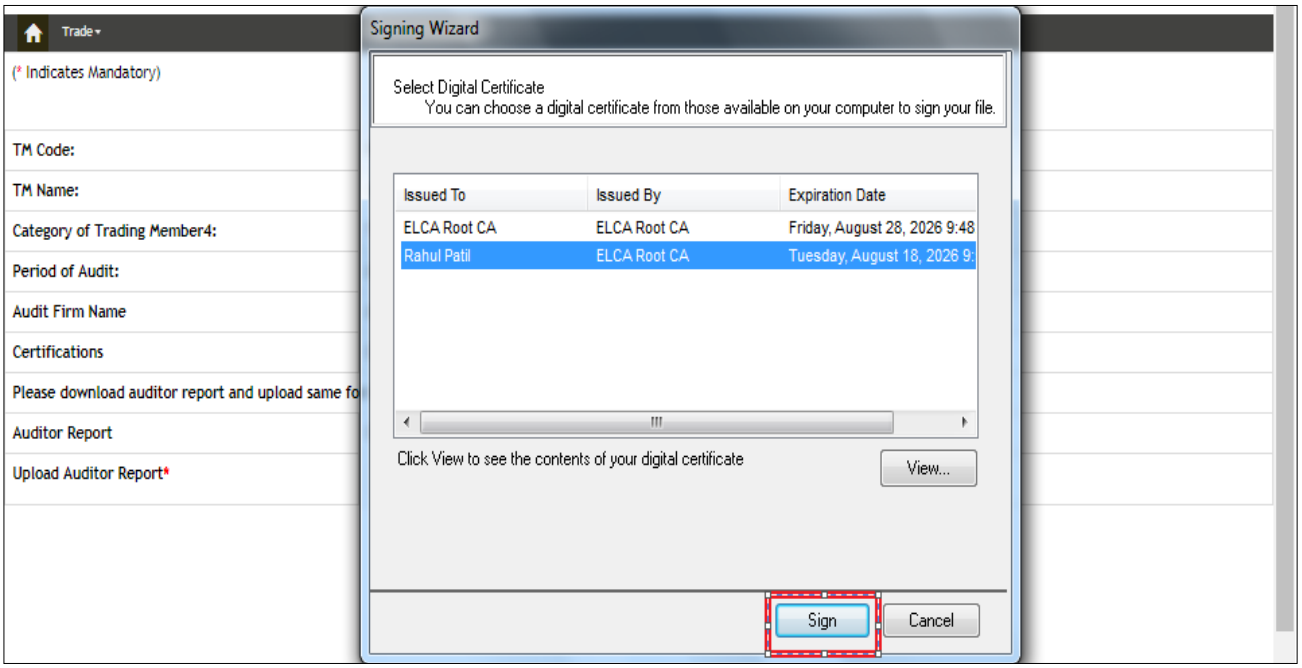
10) Click on Sign PDF button. Auditor will get below pop-up, click on Ok.



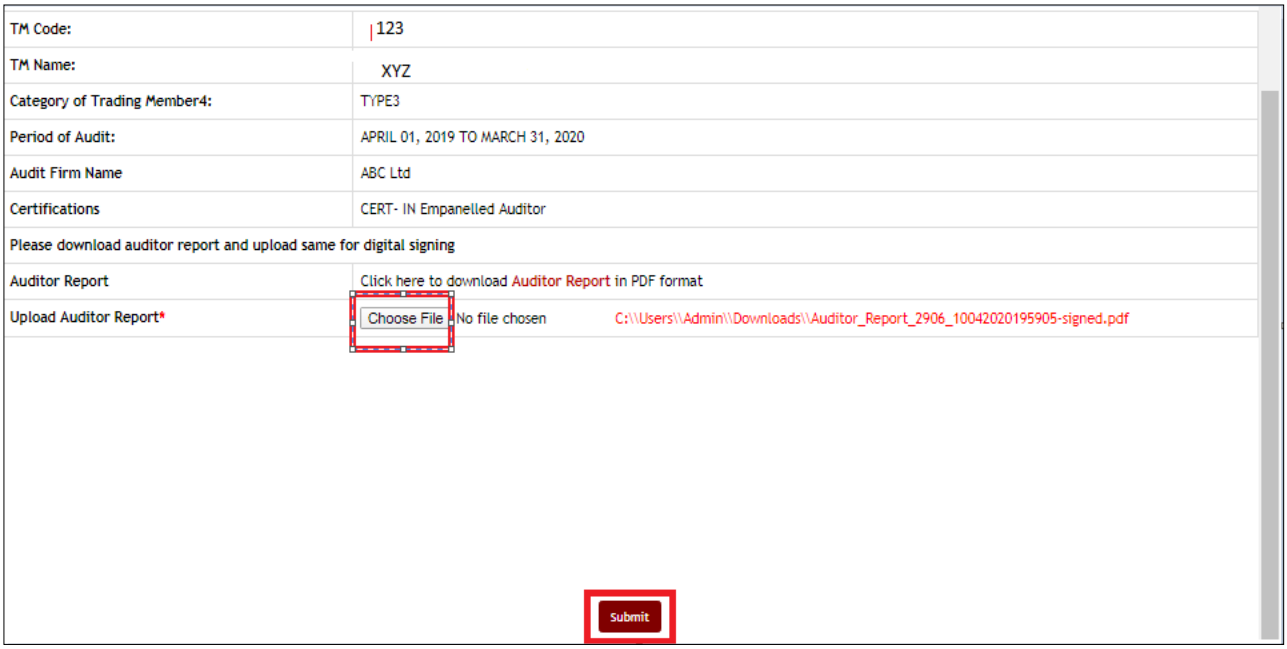
11) Click on 'Ok' for the below pop-up message. Then Auditor will be able to browse the report. Select the same PDF report which is downloaded without renaming.


www.devconnect2nse.com says
Select Auditor_Report_2906_10042020194203.pdf for signing
OK
NSE
Digital Signature Test PDF Signing
Trade
(* Indicates Mandatory)
Cyber security Audit Report Final Submission
TM Code:
90030
TM Name:
ARHAM WEALTH MANAGEMENT PVT LTD
Category of Trading Member4:
TYPE3
Period of Audit:
APRIL 01, 2019 TO MARCH 31, 2020
Audit Firm Name
ABC Ltd
Certifications
CERT- IN Empanelled Auditor
Please download auditor report and upload same for digital signing
Auditor Report
Click here to download Auditor Report in PDF format
Upload Auditor Report*
Sign PDF

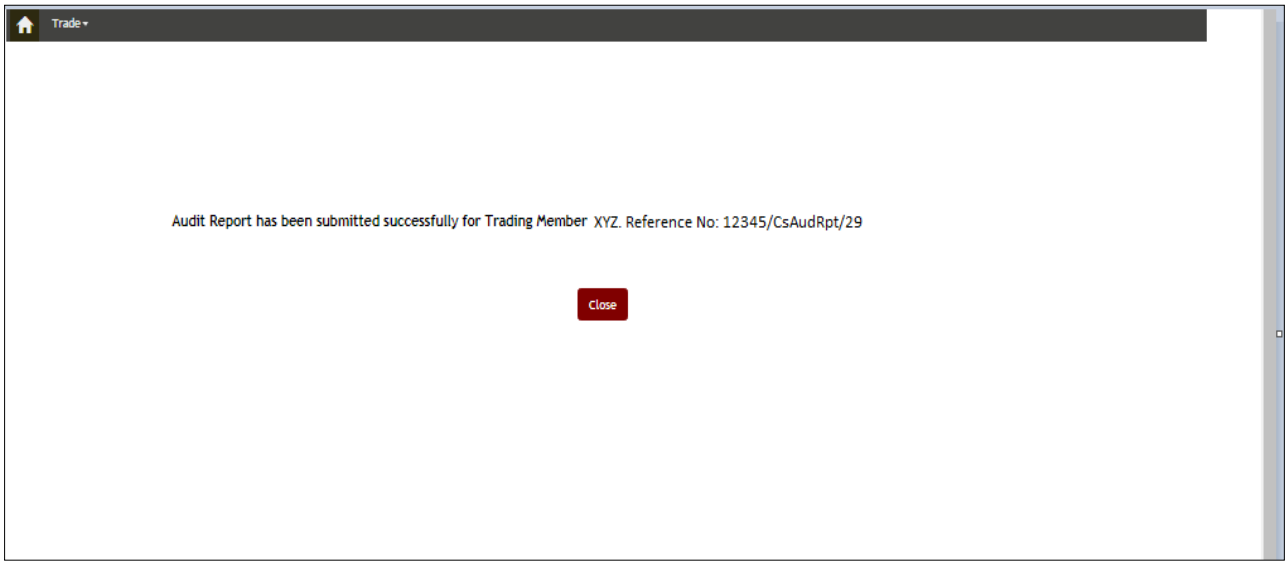
12) After browsing, Auditor will get a window for selecting Signature. Select the signature and click on ‘Sign’.



13) Save the signed file in your system and browse the same after clicking on ‘Choose File’ button. Now click on Submit button.



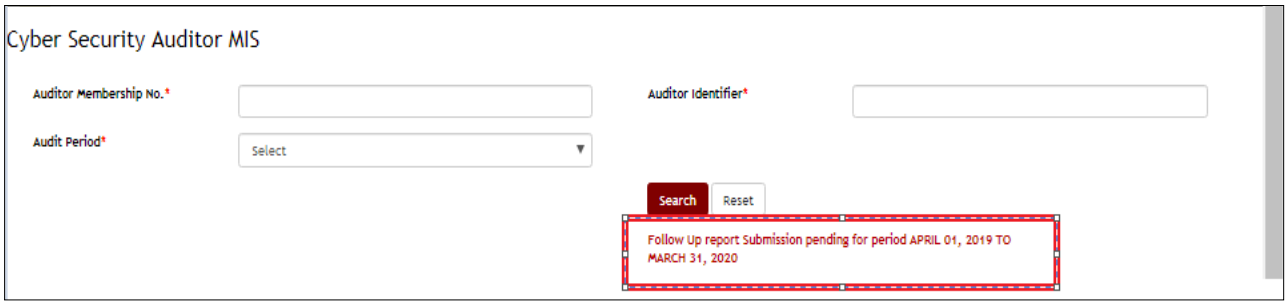
14) After submitting, Auditor will get below message.



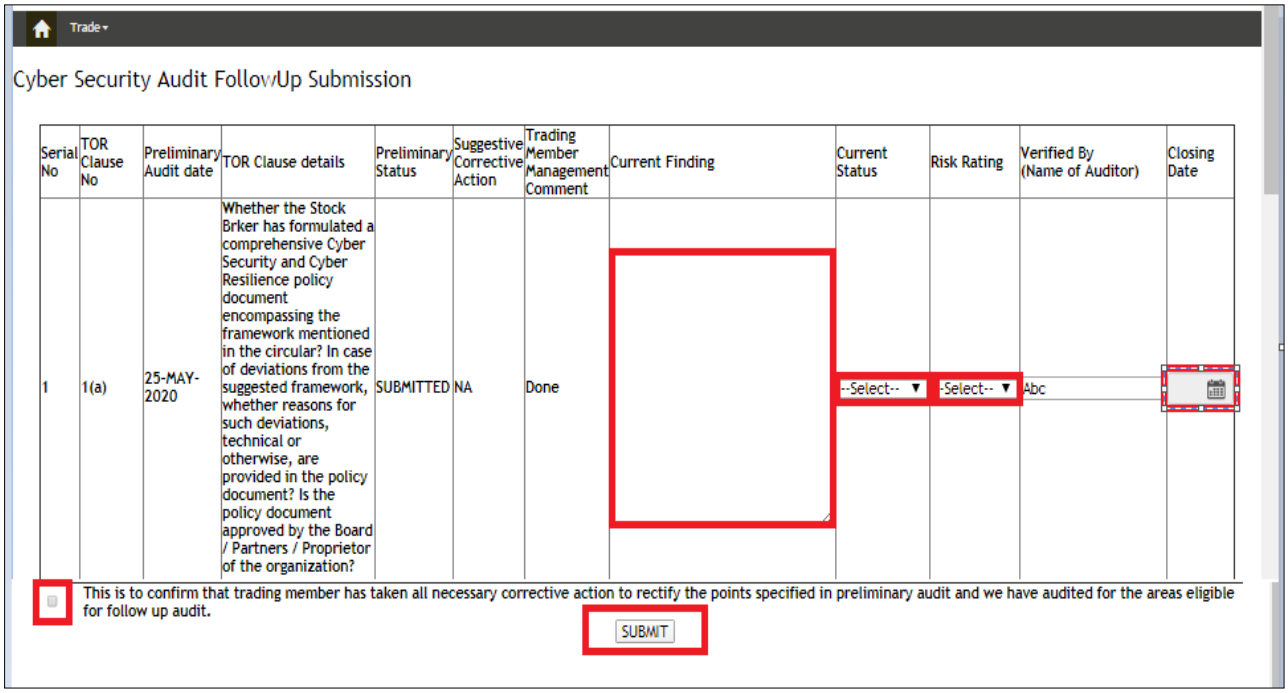
If Follow-On Audit is required, procedure given in next page is to be followed for submitting the Follow-on Audit Report.

Guidelines for submitting Follow- Up Audit Report

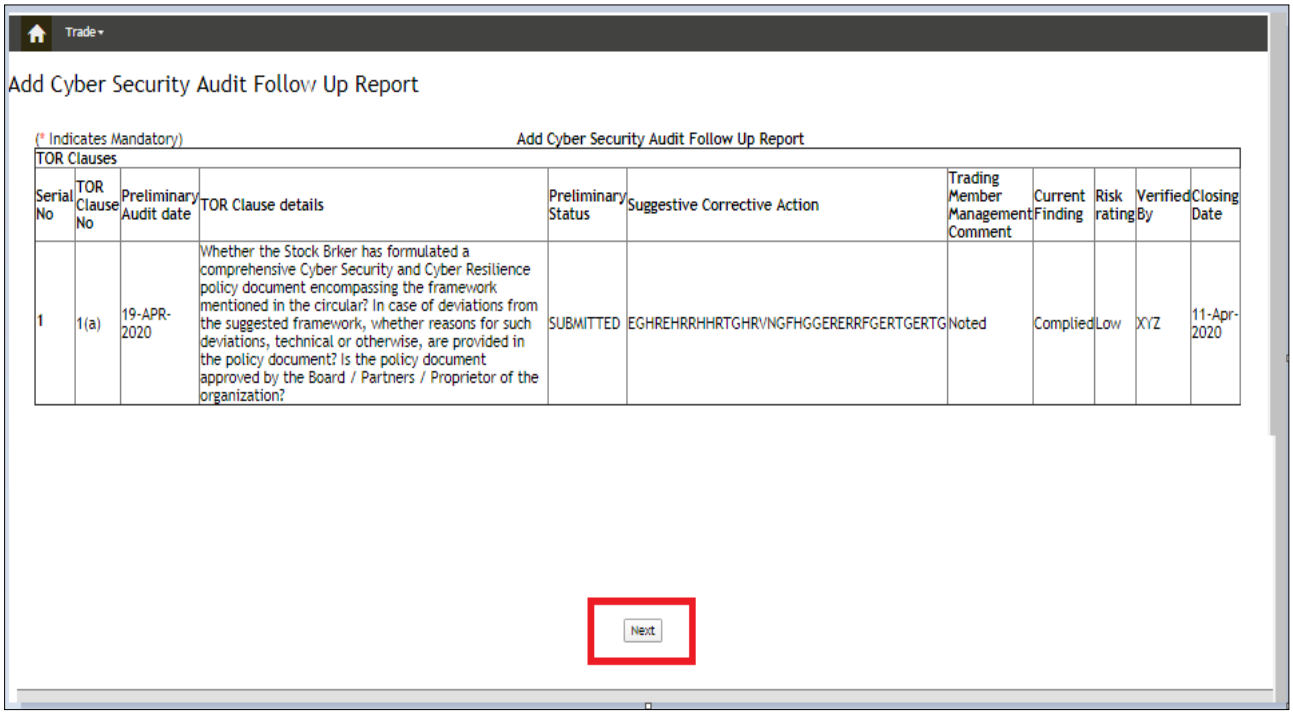
1) For submitting Follow-Up Audit, Auditor will get a link in Cyber Security Auditor MIS (Login > Enit Cyber Security > Trade > Cyber Security > Cyber Security Auditor MIS) once the Preliminary report has been submitted by Member to the Exchange.



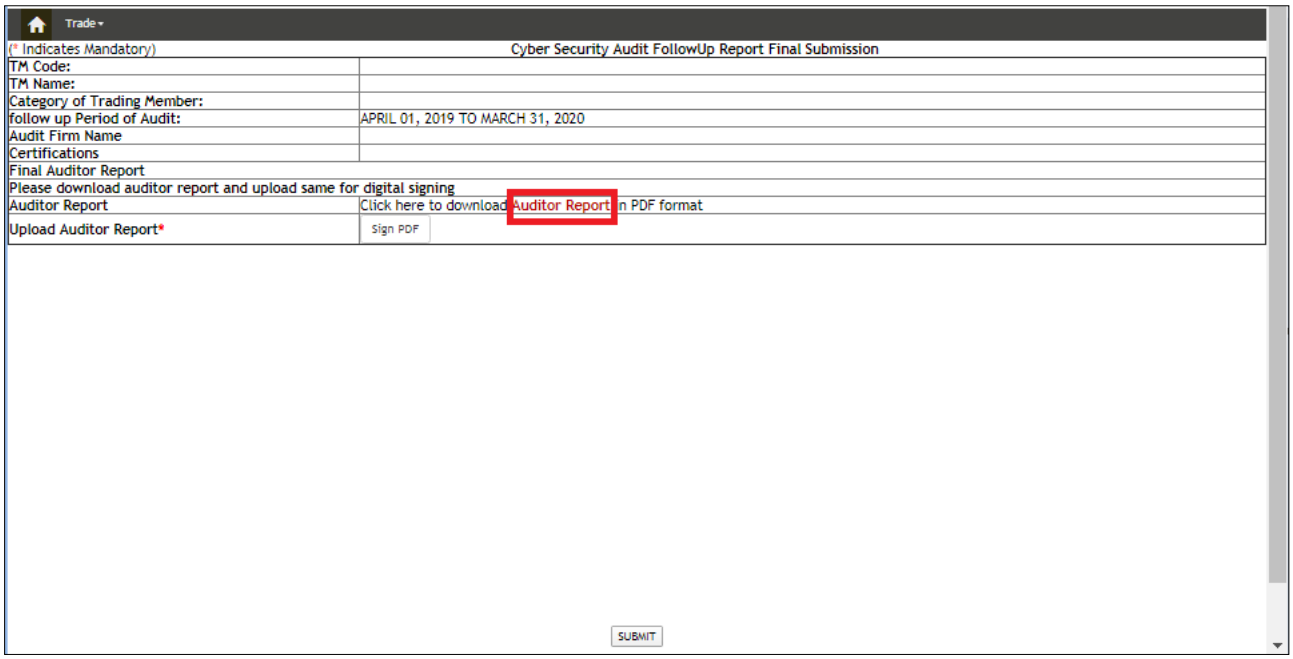
2) Fill the require details as require (Current finding, Current Status, Risk Rating, Verifying Auditor, Closing Date) > Tick on declaration checkbox > Submit.



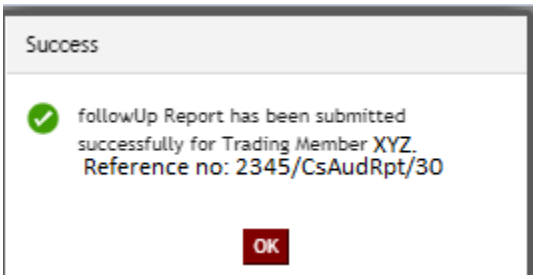
3) Click on Next button



4) Click on 'Auditor Report' link to download the PDF report.



5) Sign and upload the Follow Up Audit Report. Auditor will get below message on successfully upload of report.



Annexure – C

Auditor Selection Norms

1. The Auditor shall have minimum 3 years of experience in IT audit of securities market participants e.g. stock exchanges, clearing corporations, depositories, stock brokers, depository participants etc. The audit experience should cover all the major areas mentioned under Terms of Reference (ToR) of the system audit specified by SEBI / stock exchange.

2. Resources employed for the purpose of system audit shall have relevant industry recognized certifications e.g. CERT-IN empanelled auditor, D.I.S.A. (ICAI) Qualification , CISA (Certified Information System Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium, commonly known as (ISC).

3. The Auditor should have experience of IT audit/governance frameworks and processes conforming to industry leading practices like Cobit.

4. The Auditor shall not have any conflict of interest in conducting fair, objective and independent audit of the Trading Member. Further, the directors / partners of Auditor firm shall not be related to any stock broker including its directors or promoters either directly or indirectly.

5. The Auditor shall not have any cases pending against its previous audited companies/firms, which fall under SEBI's jurisdiction, which point to its incompetence and/or unsuitability to perform the audit task.

6. Auditor has not conducted more than 3 successive audits of the trading member. Follow-on audits conducted by the auditor shall not be considered in the successive audits.

ANNEXURE – D

Terms of Reference (TOR) for Cyber Security & Cyber Resilience audit

Clause	Details
1	**Governance**
1(a)	Whether the Stock Broker has formulated a comprehensive Cyber Security and Cyber Resilience policy document encompassing the framework mentioned in the circular? In case of deviations from the suggested framework, whether reasons for such deviations, technical or otherwise, are provided in the policy document? Is the policy document approved by the Board / Partners / Proprietor of the organisation? Whether the policy document is reviewed by the aforementioned group at least annually with the view to strengthen and improve its Cyber Security and Cyber Resilience framework.
1(b)	The Cyber Security Policy should includes the following process to identify, assess, and manage Cyber Security risk associated with processes, information, networks and systems: a. 'Identify' critical IT assets and risks associated with such assets. b. 'Protect' assets by deploying suitable controls, tools and measures. c. 'Detect' incidents, anomalies and attacks through appropriate monitoring tools/processes. d. 'Respond' by taking immediate steps after identification of the incident, anomaly or attack. e. 'Recover' from incident through incident management and other appropriate recovery mechanisms.
1(c)	The Cyber Security Policy of Stock Brokers trading through APIs based terminal / Depository Participants should consider the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organization (NTRO), Government of India (titled 'Guidelines for Protection of National Critical Information Infrastructure') and subsequent revisions, if any, from time to time.
1(d)	Stock Brokers trading through APIs based terminal / Depository Participants may refer to best practices from international standards like ISO 27001, COBIT 5, etc., or their subsequent revisions, if any, from time to time.

1(e)	Stock Brokers / Depository Participants should designate a senior official or management personnel (henceforth, referred to as the "Designated Officer") whose function would be to assess, identify, and reduce security and Cyber Security risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the Cyber Security Policy.
1(f)	Stockbrokers / Depository Participants should prepare detailed incident response plan and define roles and responsibilities of Chief Information Security Officer (CISO) and other senior personnel. Reporting and compliance requirements shall be clearly specified in the security policy. In addition, share the details of CISO with CERT-In through Email (info AT cert-in.org.in)
1(g)	Has the Board / Partners / Proprietor of the Stock Broker formed an internal Technology Committee comprising experts. This Technology Committee should on a half yearly basis review the implementation of the Cyber Security and Cyber Resilience policy approved by their Board / Partners / Proprietor, and such review should include review of their current IT and Cyber Security and Cyber Resilience capabilities, set goals for a target level of Cyber Resilience, and establish plans to improve and strengthen Cyber Security and Cyber Resilience. The review shall be placed before the Board / Partners / Proprietor of the Stock Brokers / Depository Participants for appropriate action.
1(h)	The Organization should establish a reporting procedure to facilitate communication of unusual activities and events to the Designated Officer in a timely manner.
1(i)	Does the designated officer and technology committee periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen Cyber Security and cyber resilience framework?
1(j)	Stock Broker/Depository Participant should define and document responsibilities of its employees, outsourced staff, and employees of vendors, members or participants and other entities, who may have privileged access or use systems / networks of the Stock Broker/Depository Participants towards ensuring the goal of Cyber Security ?
2	**Identification**
2(a)	Stock Brokers / Depository Participants should identify critical assets based on their sensitivity and criticality for business operations, services and data management. To this end, Stock Brokers / Depository Participants should maintain 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.

2(b)	Stock Brokers / Depository Participants should accordingly 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.
3	**Protection**
I	**Access Control**
3(a)	Any access to Stock Brokers / Depository Participants systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period. Stock Brokers / Depository Participants should grant access to IT systems, applications, databases and networks on a need-to-use basis and based on the principle of least privilege. Such access should be for the period when the access is required and should be authorized using strong authentication mechanisms.
3(b)	Stock Brokers / Depository Participants should implement an access policy which addresses strong password controls for users' access to systems, applications, networks and databases. Illustrative examples for this are given in Annexure C of SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018
3(c)	All critical systems of the Stock Broker / Depository Participant accessible over the internet should have two-factor security (such as VPNs, Firewall controls etc.)
3(d)	Stock Brokers / Depository Participants should ensure that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes. Such logs should be maintained and stored in a secure location for a time period not less than two (2) years.
3(e)	Stock Brokers / Depository Participants should deploy controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users) to Stock Broker / Depository Participant's critical systems. Such controls and measures should inter-alia include restricting the number of privileged users, periodic review of privileged users' activities, disallow privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.
3(f)	Employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to the Stock Brokers / Depository Participants critical systems, networks and other computer resources, should be subject to stringent supervision, monitoring and access restrictions.
3(g)	Stock Brokers / Depository Participants should formulate an Internet access policy to monitor and regulate the use of internet and internet based services such as social media sites, cloud-based internet storage sites, etc. within the Stock Broker / Depository Participant's critical IT infrastructure.

3(h)	User Management must address deactivation of access of privileges of users who are leaving the organization or whose access privileges have been withdrawn.
3(i)	Stock brokers/Depository Participants shall use models that take the `least privilege' approach to provide security for both on-and off-premises resources (i.e. zero-trust models).
II	**Physical Security**
3(j)	Physical access to the critical systems should be restricted to minimum and only to authorized officials. Physical access of outsourced staff/visitors should be properly supervised by ensuring at the minimum that outsourced staff/visitors are accompanied at all times by authorized employees.
3(k)	Physical access to the critical systems should be revoked immediately if the same is no longer required.
3(l)	Stock Brokers/ Depository Participants has ensured that the perimeter of the critical equipments room, if any, are physically secured and monitored by employing physical, human and procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. where appropriate
III	**Network Security Management**
3(m)	Stock Brokers / Depository Participants has established baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within their IT environment. The LAN and wireless networks should be secured within the Stock Brokers /Depository Participants' premises with proper access controls.
3(n)	For algorithmic trading facilities, adequate measures should be taken to isolate and secure the perimeter and connectivity to the servers running algorithmic trading applications.
3(o)	Stock Brokers / Depository Participants should install network security devices, such as firewalls, proxy servers, intrusion detection and prevention systems (IDS) to protect their IT infrastructure which is exposed to the internet, from security exposures originating from internal and external sources.
3(p)	Adequate controls must be deployed to address virus / malware / ransomware attacks. These controls may include host / network / application based IDS systems, customized kernels for Linux, anti-virus and anti-malware software etc.
IV	**Data Security**
3(q)	Critical data must be identified and encrypted in motion and at rest by using strong encryption methods. Illustrative measures in this regard are given in Annexure A and B of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018

3(r)	Stock Brokers / Depository Participants should implement measures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity. It should be ensured that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties. Illustrative measures to ensure security during transportation of data over the internet are given in Annexure B of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018
3(s)	The information security policy should also cover use of devices such as mobile phones, faxes, photocopiers, scanners, etc., within their critical IT infrastructure, that can be used for capturing and transmission of sensitive data. For instance, defining access policies for personnel, and network connectivity for such devices etc.
3(t)	Stockbrokers / Depository Participants should Enforce BYOD (Bring your own device) security policies, like requiring all devices to use a business-grade VPN service and antivirus protection
3(u)	Stock Brokers / Depository Participants should allow only authorized data storage devices within their IT infrastructure through appropriate validation processes.
3(v)	Stock Brokers / Depository Participants should only deploy hardened hardware / software, including replacing default passwords with strong passwords and disabling or removing services identified as unnecessary for the functioning of the system.
3(w)	Open ports on networks and systems which are not in use or that can be potentially used for exploitation of data should be blocked and measures taken to secure them.
3(x)	Stockbrokers/ Depository Participants shall deploy detection and alerting tools. Members shall create process to prevent, contain and respond to a data breach/ data leak.
V	**Application Security in Customer Facing Applications**
3(y)	Application security for Customer facing applications offered over the Internet such as IBTs (Internet Based Trading applications), portals containing sensitive or private information and Back office applications (repository of financial and personal information offered by Brokers to Customers) are paramount as they carry significant attack surfaces by virtue of being available publicly over the Internet for mass use. An illustrative list of measures for ensuring security in such applications is provided in Annexure C.
VI	**Certification of off-the-shelf products**

3(z)	Stock Brokers / Depository Participants should ensure that off the shelf products being used for core business functionality (such as Back office applications) should bear Indian Common criteria certification of Evaluation Assurance Level 4. The Common criteria certification in India is being provided by (STQC) Standardisation Testing and Quality Certification (Ministry of Electronics and Information Technology). Custom developed / in-house software and components need not obtain the certification, but have to undergo intensive regression testing, configuration testing etc. The scope of tests should include business logic and security controls.
VII	**Patch management**
3(aa)	Stock Brokers / Depository Participants should establish and ensure that the patch management procedures include the identification, categorization and prioritization of patches and updates. An implementation timeframe for each category of patches should be established to apply them in a timely manner.
3(ab)	Stock Brokers / Depository Participants should perform rigorous testing of security patches and updates, where possible, before deployment into the production environment so as to ensure that the application of patches do not impact other systems.
VIII	**Disposal of data, systems and storage devices**
3(ac)	Stock Brokers / Depository Participants should frame suitable policy for disposal of storage media and systems. The critical data / Information on such devices and systems should be removed by using methods such as crypto shredding / degauss / Physical destruction as applicable.
3(ad)	Stock Brokers / Depository Participants should formulate a data-disposal and data-retention policy to identify the value and lifetime of various parcels of data.
IX	**Vulnerability Assessment and Penetration Testing (VAPT)**
3(ae)	Stock Brokers / Depository Participants should regularly conduct vulnerability assessment to detect security vulnerabilities in their IT environments exposed to the internet.
3(af)	Stock Brokers / Depository Participants with systems publicly available over the internet should also carry out penetration tests, at-least once a year, in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks that are exposed to the internet. In addition, Stock Brokers / Depository Participants should perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system that is accessible over the internet.

3(ag)	In case of vulnerabilities discovered in off-the-shelf products (used for core business) or applications provided by exchange empanelled vendors, Stock Brokers / Depository Participants should report them to the vendors and the exchanges in a timely manner.
3(ah)	Remedial actions should be immediately taken to address gaps that are identified during vulnerability assessment and penetration testing.
4	**Monitoring and Detection**
4(a)	Stock Brokers / Depository Participants should establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events / alerts and timely detection of unauthorised or malicious activities, unauthorised changes, unauthorised access and unauthorised copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices exposed to the internet should also be monitored for anomalies.
4(b)	Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks exposed to the internet, Stock Brokers / Depository Participants should implement suitable mechanisms to monitor capacity utilization of its critical systems and networks that are exposed to the internet, for example, controls such as firewalls to monitor bandwidth usage.
5	**Response and Recovery**
5(a)	Alerts generated from monitoring and detection systems should be suitably investigated in order to determine activities that are to be performed to prevent expansion of such incident of cyber attack or breach, mitigate its effect and eradicate the incident.
5(b)	The response and recovery plan of the Stock Brokers / Depository Participants should have plans for the timely restoration of systems affected by incidents of cyber-attacks or breaches, for instance, offering alternate services or systems to Customers. Stock Brokers / Depository Participants should have the same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as specified by SEBI for Market Infrastructure Institutions vide SEBI circular CIR/MRD/DMS/17/20 dated June 22, 2012 as amended from time to time
5(c)	The response plan should define responsibilities and actions to be performed by its employees and support / outsourced staff in the event of cyber-attacks or breach of Cyber Security mechanism.
5(d)	Any incident of loss or destruction of data or systems should be thoroughly analyzed and lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes.

5(e)	Stock Brokers / Depository Participants should also conduct suitable periodic drills to test the adequacy and effectiveness of the aforementioned response and recovery plan.
6	**Sharing of Information**
6(a)	Quarterly reports containing information on cyber-attacks and threats experienced by Stock Brokers / Depository Participants and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities / threats that may be useful for other Stock Brokers / Depository Participants should be submitted to Stock Exchanges / Depositories.
7	**Training and Education**
7(a)	Stock Brokers / Depository Participants should work on building Cyber Security and basic system hygiene awareness of staff (with a focus on staff from non-technical disciplines).
7(b)	Stock Brokers / Depository Participants should conduct periodic training programs to enhance knowledge of IT / Cyber Security Policy and standards among the employees incorporating up-to-date Cyber Security threat alerts. Where possible, this should be extended to outsourced staff, vendors etc.
7(c)	The training programs should be reviewed and updated to ensure that the contents of the program remain current and relevant.
7(d)	Stockbrokers / Depository Participants should Provide training to the employees to avoid clicking on a link in a spear-phishing email, reusing their personal password on a work account, mixing personal with work email and/or work documents, or allowing someone they shouldn't to use their corporate device- especially in Work from Home environments.
8	**Systems managed by vendors**
8(a)	Where the systems (IBT, Back office and other Customer facing applications, IT infrastructure, etc.) of a Stock Brokers / Depository Participants are managed by vendors and the Stock Brokers / Depository Participants may not be able to implement some of the aforementioned guidelines directly, the Stock Brokers / Depository Participants should instruct the vendors to adhere to the applicable guidelines in the Cyber Security and Cyber Resilience policy and obtain the necessary self-certifications from them to ensure compliance with the policy guidelines.
9	**Cyber Security Advisory – Standard Operating Procedure (SOP) for handling cyber security incidents of intermediaries-as per SEBI directives**

9(a)	The stock brokers should formulate Standard Operating Procedure and adhere with the SOP for handling and reporting of Cyber Security Incidents. The aspects which shall form part of the SOP and which needs to be complied with by stock Brokers should be as per Exchange circular NSE/INSP/48163 dated May 03, 2021

*****End of Document*****