

National Stock Exchange of India Limited

Circular

DEPARTMENT: INSPECTION	
Download Ref No: NSE/INSP/53992	Date: October 07, 2022
Circular Ref. No: 75/2022	

To All Members,

Subject: Cyber Security and Cyber Resilience Audit of Trading Members (Type-III)

In accordance with 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, SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022 and SEBI/HO/MIRSD/TPD/P/CIR/2022/93 dated June 30, 2022 in relation to Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants, trading members using algorithm software (Type – III) are required to conduct cyber security and cyber resilience audit for the period April 01, 2022 to September 30, 2022 and submit the report to the Exchange as per the following timelines

Audit Period	Last date for Submission		
	Preliminary Audit Report	Action Taken Report (ATR) (If applicable)	Follow-on Audit Report (if applicable)
Half Yearly (April 22- September 22)	November 30, 2022	February 28, 2023,	May 31, 2023,

The link for the submission of Cyber Security Audit report will be available from October 14, 2022. The procedure for submitting the report by member and auditor through ENIT module in the Member portal is provided in **Annexure- A** and **Annexure-B** respectively.

Submission of Cyber Security and Cyber Resilience audit report shall be considered complete 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 and Cyber Resilience Audit Report.

Penalty/disciplinary actions	Penalty/disciplinary action in case of Repeat violation/contravention
<ol style="list-style-type: none"> For 1st week after due date, Charges of Rs. 2,500/- per day Charges of Rs. 5000/- per day from second week after due date In case of non-submission within three weeks from the due date of submission, new client registration to be prohibited and notice of 7 days for disablement of trading facility till submission of data/report. The disablement notice issued to the member shall be shared with all the Exchanges for information. In case of non-submission within four weeks from the due date of submission, Member shall be disabled in all segments till submission of data/report. 	<p>In case of a repeat instance by the Member, levy of applicable monetary penalty along with an escalation of 50%.</p> <p>In case of non-submission for within three weeks from the due date of submission, new client registration to be prohibited and notice of 7 days for disablement of trading facility till submission of data/report.</p> <p>The disablement notice issued to the member shall be shared with all the Exchanges for information. In case of non-submission within four weeks from the due date of submission, Member shall be disabled in all segments till submission of data/report.</p>

Trading members shall comply with any non-compliance/ non-conformities (NCs) pending for Cyber Security and Cyber Resilience Audit Report for the previous audit period by submitting ATR and/or Follow-on audit report as the case may be through ENIT.

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

For and on behalf of
National Stock Exchange of India Limited

Ajinkya Nikam
Senior Manager-Inspection

Enclosure

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

Annexure B – User guide for Auditor to submit Cyber Security Audit Report.

Annexure C – Auditor Selection Norms.

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

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

Regional Office	CONTACT NO.	E MAIL ID
Ahmedabad (ARO)	079-49008632	inspectionahm@nse.co.in
Chennai (CRO)	044- 66309915/17	inspection_cro@nse.co.in
Delhi (DRO)	011-23459127 / 38 / 46	delhi_inspection@nse.co.in
Kolkata (KRO)	033-40400411 / 06	inspection_kolkata@nse.co.in
Mumbai (WRO)	022- 25045264/259/224	compliance_wro@nse.co.in
Central Help Desk	compliance_assistance@nse.co.in	

Annexure A

User guide to submit Cyber Audit for Member

A) Registration of Auditor

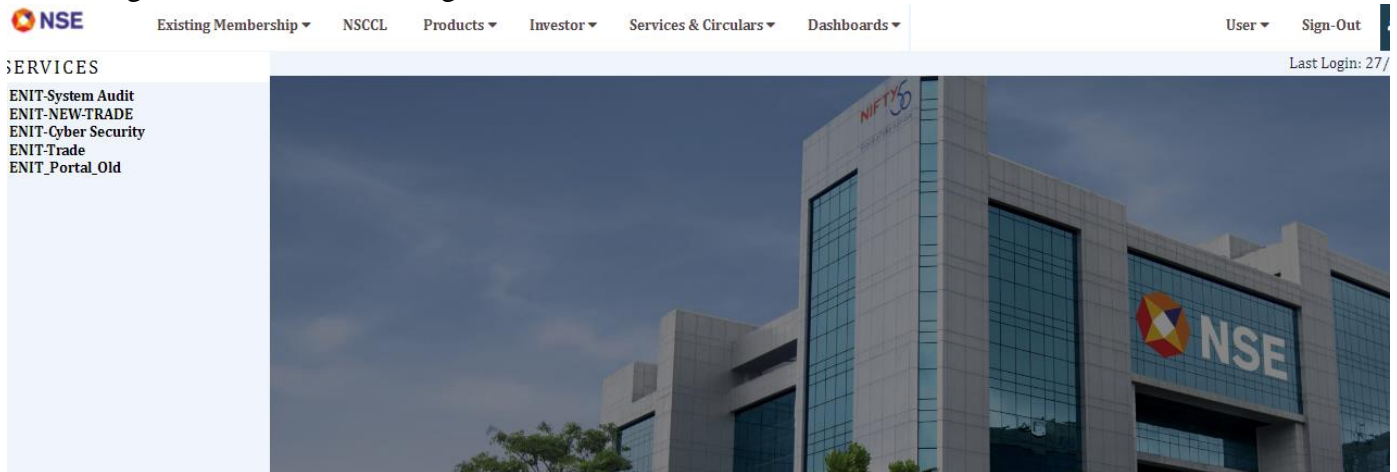
- 1) Admin User need to create 2 user ids in Member Portal.
 - a) One user id for the user at member's end who will register Auditor and submit the final Audit Report from member's end. Here Admin will assign '**ENIT- NEW-TRADE**' role to user.

[illegible]

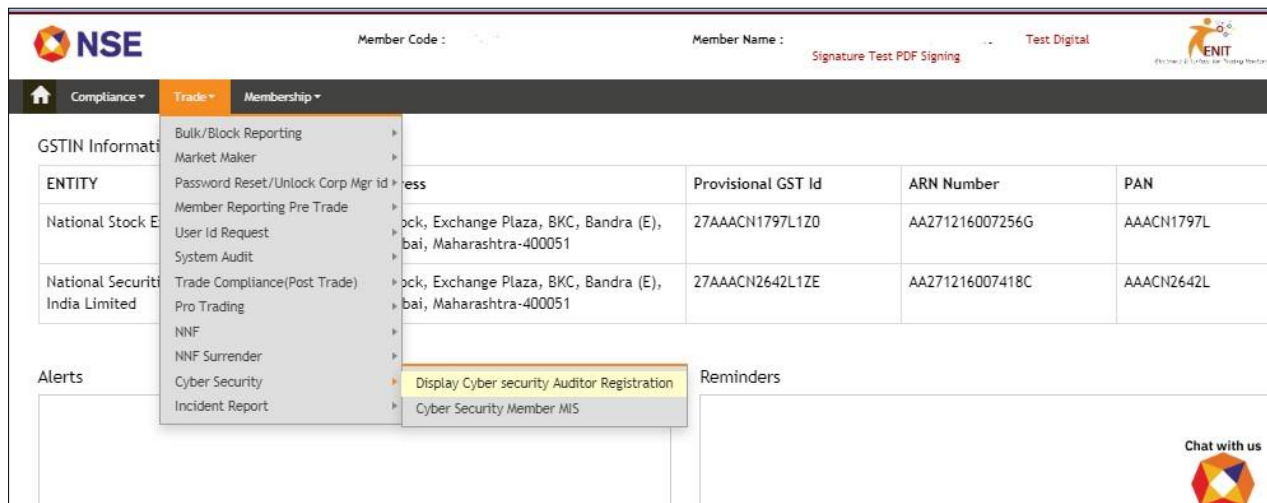
- b) Then second user id is to be created for Auditor. Here Admin will assign ‘**ENIT-Cyber Security**’ role to Auditor

[illegible]


- 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.



Member Code :

Member Name :
Digital Signature Test PDF Signing

Test


Electronic & Surface for Trading Members

[Home](#) [Compliance](#) [Trade](#) [Membership](#)

Cyber Security Auditor Registration

New Auditor

S.No	Audit Period	Auditor Login Id	Auditor Membership No	Firm Name	Auditor Name	Audit Firm Registration No	Qualification	Email Id	Created Date	Update Auditor Entry	Delete Auditor Entry
------	--------------	------------------	-----------------------	-----------	--------------	----------------------------	---------------	----------	--------------	----------------------	----------------------

NSE Copyright (c) 2016

5) Fill the details for Auditor Registration.

Add Cyber Security Auditor

Audit Period*

Select

Member Category*

Auditor Login Id*

Auditor Password*

Auditor Membership No*

Auditor Firm Name*

Auditor Name*

Audit Firm Registration No*

Auditor Qualification*

☐ DISA ☐ CISA ☐ CISM ☐ CISSP ☐ CERT-IN Empanelled Auditor

Auditor Email Id*

We undertake that we have verified the following points:

☐ The Auditor has 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 covers all the

- 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.

The screenshot shows the 'Add Cyber Security Auditor' form. A modal window is displayed with a warning icon and the following text: 'Note: Make sure your chosen audit Period is from oldest to latest. for example assume we have the following audit period (OCTOBER 01, 2013 TO MARCH 31, 2014) and (APRIL 01, 2014 TO SEPTEMBER 30, 2014). Here you have to choose (OCTOBER 01, 2013 TO MARCH 31, 2014) audit period.' The modal has an 'Ok' button. The form in the background has fields for 'Audit Period*', 'Auditor Login Id*', 'Auditor Membership No*', and 'Auditor Name*'. The 'Audit Period*' field is currently set to 'APRIL 01, 2014 TO SEPTEMBER 30, 2014'.

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

The screenshot shows the 'Add Cyber Security Auditor' form. A modal window is displayed with a warning icon and the following text: 'Kindly confirm that login id created in member portal for auditor matches with the login id provided here'. The modal has 'Yes' and 'No' buttons. The form in the background has fields for 'Audit Period*', 'Auditor Login Id*', 'Auditor Membership No*', 'Auditor Name*', 'Auditor Qualification*', 'Auditor Password*', 'Auditor Firm Name*', 'Audit Firm Registration No*', and 'Auditor Email Id*'. The 'Audit Period*' field is currently set to 'APRIL 01, 2018 TO MARCH 31, 2019'. The 'Auditor Login Id*' field is currently set to 'EnitUr290030'. The 'Auditor Qualification*' field has radio buttons for 'DISA', 'CISA', 'CISM', 'CISSP', and 'CERT-IN Empanelled Auditor'. The 'Auditor Qualification*' field is currently set to 'DISA'. The 'Auditor Qualification*' field has a note: 'NOTE: Trading members may note that the category / period of audit is indicative, who are depository participants or are involved in offering any other financial service. Do you want to change the category and period of audit provided? Verify'. The 'Auditor Qualification*' field has a note: 'We undertake that we have verified the following points:'. The 'Auditor Qualification*' field has a note: 'For No NSE/CMTR/26285 dated 25th March, 2014. For trading members contact exchange at 1900220053'.

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

The screenshot shows a registration form for an auditor. The form fields are as follows:

Auditor Login Id*	EnitUser190030	Auditor Password*	Nse@12345
Auditor Membership No*	123456	Auditor Firm Name*	ABC Ltd
Auditor Name*	ABC		12345678
Auditor Qualification*	<input type="radio"/> DISA <input type="radio"/> CISA <input type="radio"/> CISM <input type="radio"/> CISSP <input type="radio"/> CERT		
We undertake that we have verified the following points: <input checked="" type="checkbox"/> The Auditor has 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 covers all the major areas mentioned under Terms of Reference (ToR) of the system audit specified by SEBI / stock exchange. <input checked="" type="checkbox"/> The Auditor has experience of IT audit/governance frameworks and processes conforming to industry leading practices like CobIT <input checked="" type="checkbox"/> The Auditor does not have any conflict of interest in conducting fair, objective and independent audit of the Stock Broker. Further, the directors / partners of Auditor firm are not related to us including its directors or promoters either directly or indirectly. <input checked="" type="checkbox"/> The Auditor does 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.			

A warning pop-up is displayed in the center of the form:

⚠ Kindly note only one auditor can be registered for one period.

Ok

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

Cyber Security Auditor Registration

S.No	Audit Period	Auditor Login Id	Auditor Membership No	Firm Name	Audit Firm	Qualification	Email Id	Created Date	Update Auditor Entry
1	APRIL 01, 2018 TO MARCH 31, 2019	EnitUr390030	123456	ABCLtd			hrawat@nse.co.in	08-Apr-2020 12:49:48 AM	Update

A warning pop-up is displayed in the center of the table:

Warning

⚠ Auditor Registration Done Successfully.

Ok

NSE Copyright (c) 2016

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.

The screenshot shows the NSE ENIT-NEW-TRADE web application. The 'Trade' menu is expanded, showing options like Bulk/Block Reporting, Market Maker, Password Reset, etc. The 'Cyber Security Member MIS' option is highlighted in yellow. The background shows a table with member details and a 'Reminders' section.

- 2) Select period and click on Search button

The screenshot shows the 'Cyber Security Member MIS Report' form. The 'Member Name' is 'XYZ', 'Member Code' is '90030', and 'Audit Period' is 'APRIL 01, 2019 TO MARCH 31, 2020'. The 'Search' button is highlighted in red.

- 3) Click on Reference No. link

The screenshot shows the 'Cyber Security Member MIS Report' table. The 'Reference No.' link is highlighted in red. The table contains the following data:

Sr. No.	Reference No.	ATR Pending	Member Code	Member Name	Member Category	Audit Report Period	Auditor Firm Name	Auditor Qualification	Status of Preliminary Audit Report	Audit Compl Status
1	90030/CsAudBpt/29	X	90030	ARHAM WEALTH MANAGEMENT PVT LTD	TYPE3	APRIL 01, 2019 TO MARCH 31, 2020	ABC Ltd	CERT- IN Empanelled Auditor	SUBMITTED TO MEMBER	

- 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.

Add Cyber Security Audit Report	
TM Code:	12345
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
Contact Person Details*	<div>Contact Person Name Manoj</div> <div>Contact Person Mobile No 4563453546</div> <div>Contact Person Email manoj@member.com</div>
Status of Report Submitted	SUBMITTED TO MEMBER
Cyber Security Audit Report Submitted By Auditor	Click here to download Cyber Security Audit Report Submitted By Auditor
Auditor Report Upload*	<div>Choose File No file chosen</div>
<div>Submit</div>	

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

Certifications	CERT- IN Empanelled Auditor
Contact Person Details*	<div>Contact Person Name Manoj</div> <div>Contact Person Mobile No 4563453546</div> <div>Contact Person Email manoj@member.com</div>
Status of Report Submitted	SUBMITTED TO MEMBER
Cyber Security Audit Report Submitted By Auditor	Click here to download Cyber Security Audit Report Submitted By Auditor
Auditor Report Upload*	<div>Choose File Auditor_Rep...29digi.xlsx</div> <div>Submit</div>

- 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.

Compliance Trade Membership

(* Indicates Mandatory)

Add Cyber Security Audit Member Report

☐

TOR Clauses

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 Anlysis
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.

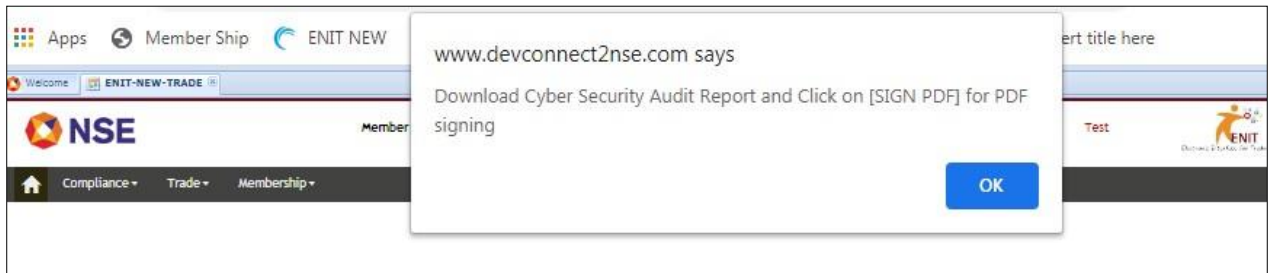
Welcome ENIT-NEW-TRADE

	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	FDWFEWE154685	IT	Not Applicable	Not Applicable	DFGGRGRTGRTGRTTGRTHRHRTHRHRHRH
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	FDWFEWE154685	IT	Not Applicable	Not Applicable	DFGGRGRTGRTGRTTGRTHRHRTHRHRHRH

Next

NSE Copyright (c) 2016

8) Click 'Ok' on pop-up message



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

A screenshot of the 'Cyber Security Audit Report Final Submission' form. The form contains the following fields:

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](#)

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*

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

Trade

(* Indicates Mandatory)

TM Code:

TM Name:

Category of Trading Member:

Period of Audit:

Audit Firm Name

Certifications

Please download auditor report and upload same for

Audit Report

Upload Audit Report*

Signing Wizard

Select Digital Certificate
You can choose a digital certificate from those available on your computer to sign your file.

Issued To	Issued By	Expiration Date
ELCA Root CA	ELCA Root CA	Friday, August 28, 2026 9:48

Click View to see the contents of your digital certificate

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

Code:	123
TM Name:	XYZ
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	
Audit Report	Click here to download Auditor Report in PDF format
Upload Audit Report*	<div>Choose File No file chosen C:\Users\Admin\Downloads\Auditor_Report_2906_10042020195905-signed.pdf</div>
<div>Submit</div>	

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

Compliance + Trade + Membership +

Cyber Security Member MIS Report

Member NameXYZMember Code90030Req Ref No

Status of Preliminary Audit ReportSelectAudit PeriodAPRIL 01, 2019 TO MARCH 31, 2020

SearchReset

Export

Sr. No.	Reference No.	ATR Pending	Member Code	Member Name	Member Category	Audit Report Period	Auditor Firm Name	Auditor Qualification	Status of Preliminary Audit Report	Audit Compl Status
1	90030/CsAudRpt/29	click Here to submit ATR	90030	ARHAM WEALTH MANAGEMENT PVT LTD	TYPE3	APRIL 01, 2019 TO MARCH 31, 2020	ABC Ltd	CERT- IN Empanelled Auditor	SUBMITTED TO EXCHANGE	

- 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.

Compliance Trade Membership

Cyber Security Member MIS Report

Member Name: XYZ Member Code: 90030 Req Ref No:

Status of Preliminary Audit Report: Select Audit Period: APRIL 01, 2020 TO SEPTEMBER 30, 2020

[Search](#) [Reset](#)

Export:

Sr. No.	Reference No.	ATR Pending	Member Code	Member Name	Member Category	Audit Report Period	Auditor Firm Name	Auditor Qualification	Status of Preliminary Audit Report	Audit Compli Status
1	90030/CsAudRpt/30	click Here to submit ATR	90030	ARHAM WEALTH MANAGEMENT PVT LTD	TYPE3	APRIL 01, 2020 TO SEPTEMBER 30, 2020	WXYZ	CERT- IN Empanelled Auditor	SUBMITTED TO EXCHANGE	

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

Welcome ENIT-NEW-TRADE

Compliance Trade Membership

Cyber Security Audit ATR Submission

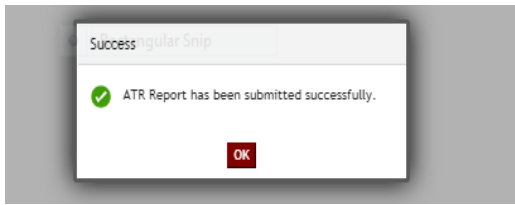
TOR Clause No	TOR Description	Description Of Finding	Status Of Finding Reported By Auditor	Risk rating Reported By Auditor	Suggestive Corrective Action	Trading Member Management Comment	Revised Status of Finding	Revised Risk Rating	Exceptions To Be Notified If Any
1(b)	The Cyber Security Policy should 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.	FDWEFWE154685	Non Compliant	Medium Risk	EGHREHRRHRTGHRVNGFHGGERERRFGERTGERTG	Noted	Compliant	Low	*NEAT NOW FOW

This is to confirm that we have taken satisfactory corrective action to rectify all the areas which has been rated as medium/weak by the Cyber Security auditor. Also, the Action Taken Report (ATR) for the same has been duly certified by the Cyber Security auditor.

[Submit Atr Details](#)

NSE Copyright (c) 2016

16) Below message after successful submission.

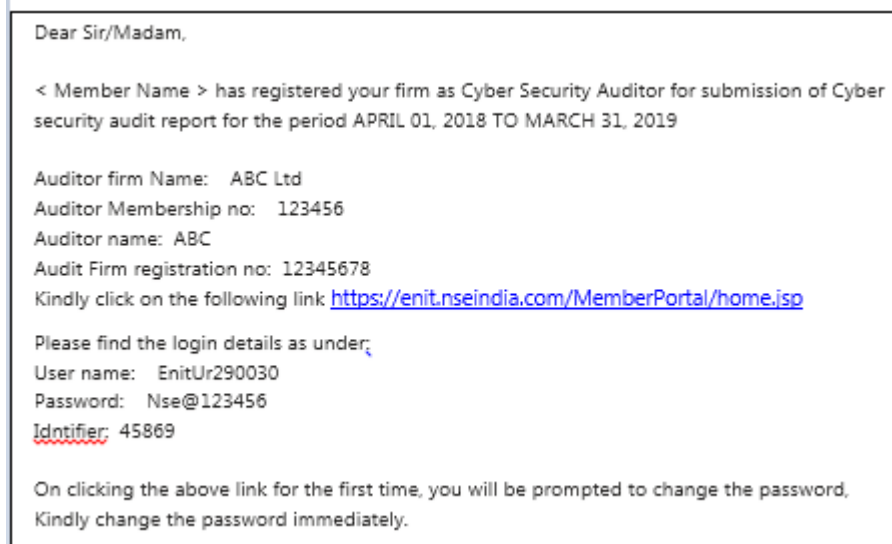


*****END OF DOCUMENT*****

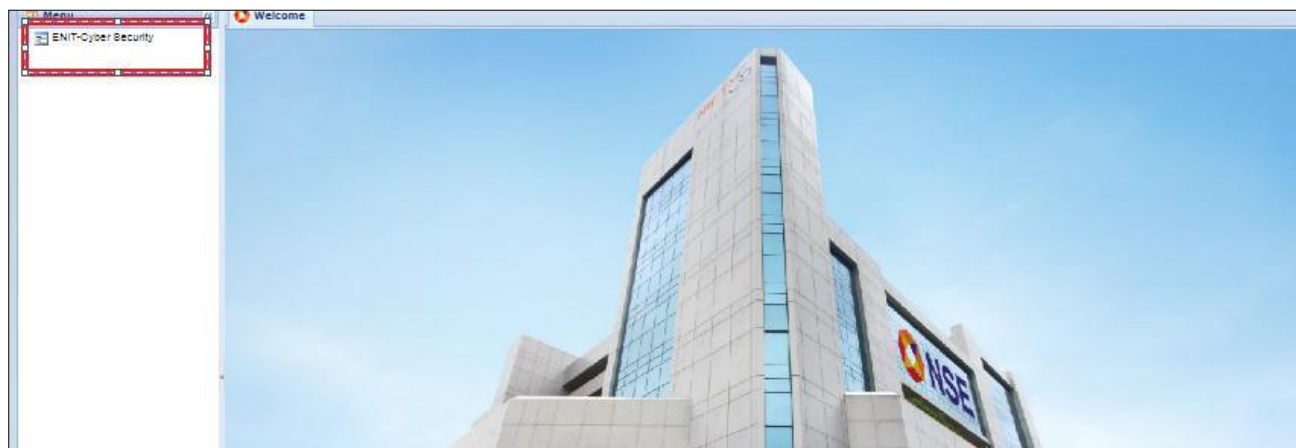
Annexure B

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



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



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

The screenshot shows the NSE ENIT Cyber Security Auditor MIS interface. The page has a header with the NSE logo and a navigation menu. The 'Cyber Security Auditor MIS' menu item is highlighted. Below the menu, there is a table with two rows of entity data.

ENTITY	Address	Provisional GST Id	ARN Number
National Stock Exchange of India Limited	G-Block, Exchange Plaza, BKC, Bandra (E), Mumbai, Maharashtra-400051	27AAACN1797L1Z0	AA27121600725
National Securities Clearing Corporation of India Limited	G-Block, Exchange Plaza, BKC, Bandra (E), Mumbai, Maharashtra-400051	27AAACN2642L1ZE	AA27121600741

Below the table, there are sections for 'Alerts' and 'Reminders'.

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

The screenshot shows the 'Cyber Security Auditor MIS' form. The form has three input fields: 'Auditor Membership No.' with the value '123456', 'Auditor Identifier' with the value '34013', and 'Audit Period' with the value 'APRIL 01, 2019 TO MARCH 31, 2020'. There are 'Search' and 'Reset' buttons. The 'New Report' button is highlighted with a red box.

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.

TM Code:	90030
TM Name:	ARHAM WEALTH MANAGEMENT PVT LTD
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
Contact Person Details*	Contact Person Name <input type="text" value="ABC"/> Contact Person Mobile No <input type="text" value="7123858454"/> Contact Person Email <input type="text" value="hrawat@nse.co.in"/>
Auditor Report Template	<div style="border: 1px solid red; padding: 2px;"> Auditor Report Template 1) Kindly download latest template. 2) Avoid copy paste of values from one template to another template. 3) Avoid copy paste in fields containing dropdown values. 4) Date format should be dd-Mon-yyyy (example: 02-May-2014). 5) Kindly provide value as NA for Fields which are not applicable. </div>
Auditor Report Upload*	<input type="button" value="Choose File"/> No f...sen

- 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'.

TM Code:	90030
TM Name:	ARHAM WEALTH MANAGEMENT PVT LTD
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
Contact Person Details*	Contact Person Name <input type="text" value="ABC"/> Contact Person Mobile No <input type="text" value="7123858454"/> Contact Person Email <input type="text" value="hrawat@nse.co.in"/>
Auditor Report Template	<div style="border: 1px solid red; padding: 2px;"> Auditor Report Template 1) Kindly download latest template. 2) Avoid copy paste of values from one template to another template. 3) Avoid copy paste in fields containing dropdown values. 4) Date format should be dd-Mon-yyyy (example: 02-May-2014). 5) Kindly provide value as NA for Fields which are not applicable. </div>
Auditor Report Upload*	<input type="button" value="Choose File"/> No f...sen
	<input type="button" value="Email"/>
	<input type="button" value="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.

- 8) Click on next button

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

The screenshot shows the NSE ENIT portal interface. A pop-up window is displayed with the text: "Download Cyber Security Audit Report and Click on [SIGN PDF] for PDF signing". The "OK" button in the pop-up is highlighted with an orange box. Below the pop-up, the main form contains the following details:

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
Actual Audit Period*	
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*	<input type="button" value="Sign PDF"/> <input type="button" value="Choose File"/> No file chosen

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

The screenshot shows the NSE ENIT portal interface after clicking the "Sign PDF" button. A pop-up window is displayed with the text: "Select Auditor_Report_2906_10042020192315.pdf for signing". The "OK" button in the pop-up is highlighted with a blue box. Below the pop-up, the main form contains the following details:

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*	<input type="button" value="Sign PDF"/>

10) 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.

The screenshot shows a web browser window with the NSE (National Securities Exchange of India) website. A pop-up message from www.devconnect2nse.com is displayed, asking the user to select a PDF report for signing. The pop-up has an 'OK' button highlighted with a red dashed border. The background website shows a form titled 'Cyber security Audit Report Final Submission' with various fields for trading member information and audit details. A 'Sign PDF' button is visible at the bottom of the form.

www.devconnect2nse.com says

Select Auditor_Report_2906_10042020194203.pdf for signing

OK

Trade

(* Indicates Mandatory)

Cyber security Audit Report Final Submission

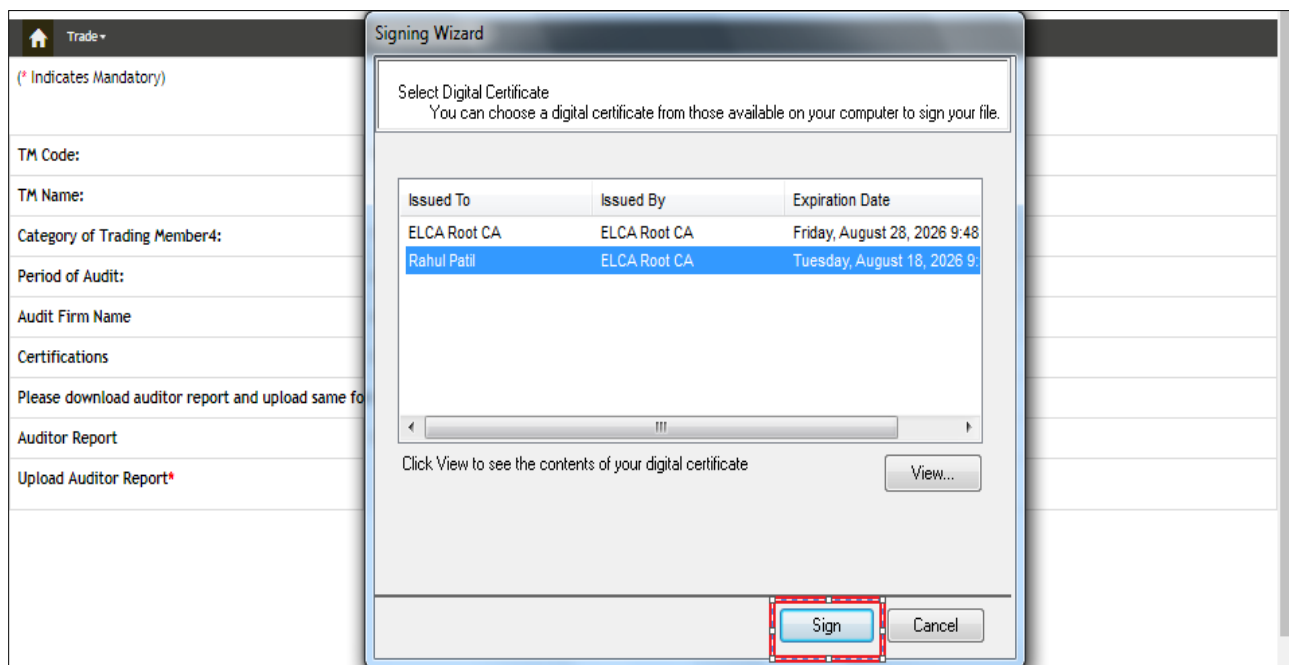
TM Code:	90030
TM Name:	ARHAM WEALTH MANAGEMENT PVT LTD
Category of Trading Member4:	TYPE3
Period of Audit:	APRIL 01, 2019 TO MARCH 31, 2020
Audit Firm Name	ABC Ltd
Certifications	CERT- IN Empanelled Auditor

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

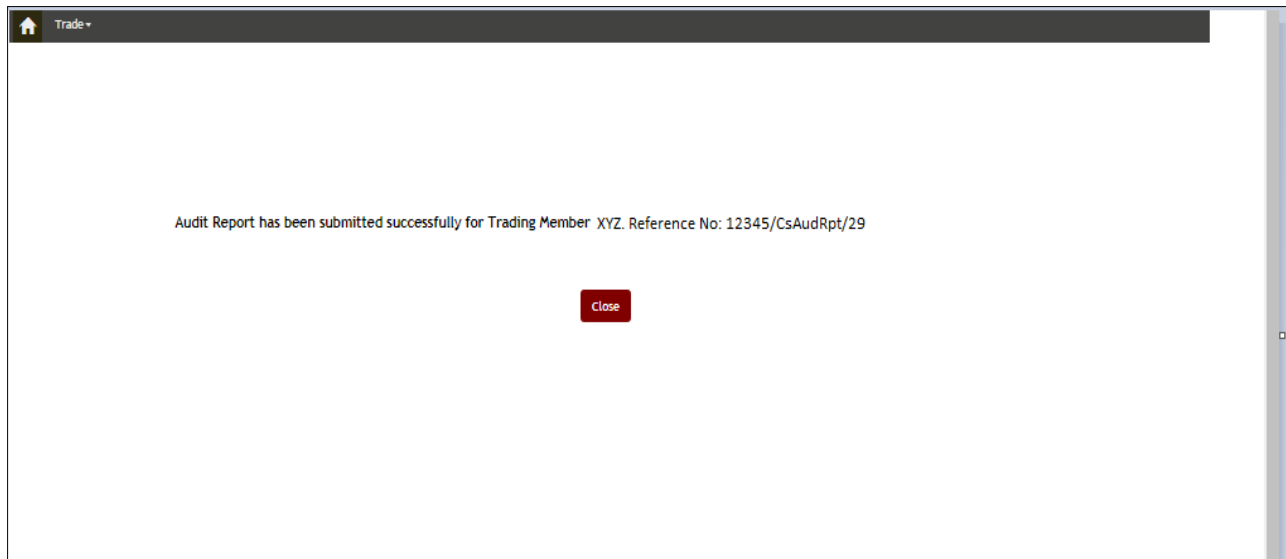
After browsing, Auditor will get a window for selecting Signature. Select the signature and click on 'Sign'.



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

TM Code:	123
TM Name:	XYZ
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*	<div>Choose File</div> <div>No file chosen</div> <div>C:\Users\Admin\Downloads\Auditor_Report_2906_10042020195905-signed.pdf</div>
<div>Submit</div>	

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.

Cyber Security Auditor MIS

Auditor Membership No.*

Auditor Identifier*

Audit Period*

Follow Up report Submission pending for period APRIL 01, 2019 TO MARCH 31, 2020

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

Trade ▾

Cyber Security Audit FollowUp Submission

Serial No	TOR Clause No	Preliminary Audit date	TOR Clause details	Preliminary Status	Suggestive Corrective Action	Trading Member Management Comment	Current Finding	Current Status	Risk Rating	Verified By (Name of Auditor)	Closing Date
1	1(a)	25-MAY-2020	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 organization?	SUBMITTED	NA	Done		--Select-- ▾	--Select-- ▾	Abc	<input type="button" value="Close"/>

☐ This is to confirm that trading member has taken all necessary corrective action to rectify the points specified in preliminary audit and we have audited for the areas eligible for follow up audit.

3) Click on Next button

Trade

Add Cyber Security Audit Follow Up Report

(* Indicates Mandatory)

Serial No	TOR Clause No	Preliminary Audit date	TOR Clause details	Preliminary Status	Suggestive Corrective Action	Trading Member Management Comment	Current Finding	Risk rating	Verified By	Closing Date
1	1(a)	19-APR-2020	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 organization?	SUBMITTED	EGHREHRRHRTGHRVNGFHGGERERRFGERTGERTG	Noted	Complied	Low	XYZ	11-Apr-2020

[Next](#)

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

Trade

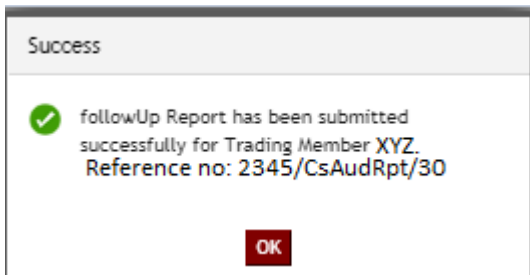
Cyber Security Audit FollowUp Report Final Submission

(* Indicates Mandatory)

TM Code:	
TM Name:	
Category of Trading Member:	
Follow up Period of Audit:	APRIL 01, 2019 TO MARCH 31, 2020
Audit Firm Name	
Certifications	
Final Auditor Report	
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

[SUBMIT](#)

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



****End Of Document****

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, stockbrokers, 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 Cyber Security 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)	<p>Whether the Stock Broker has formulated a comprehensive Cyber Security and Cyber Resilience policy document encompassing the framework mentioned in the circular?</p> <p>In case of deviations from the suggested framework, whether reasons for such deviations, technical or otherwise, are provided in the policy document?</p> <p>Is the policy document approved by the Board / Partners / Proprietor of the organisation?</p> <p>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.</p>
1(b)	<p>The Cyber Security Policy should includes the following process to identify, assess, and manage Cyber Security risk associated with processes, information, networks and systems:</p> <ul style="list-style-type: none">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)	<p>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.</p>
1(d)	<p>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.</p>

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)	<p>Has the Board / Partners / Proprietor of the Stock Broker formed an internal Technology Committee comprising experts.</p> <p>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.</p>
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)	<p>Has the Stock Broker / Depository Participant identified and classified critical assets based on their sensitivity and criticality for business operations, services and data management.</p> <p>The critical assets shall include business critical systems, internet facing applications /systems, systems that contain sensitive data, sensitive personal data, sensitive financial data, Personally Identifiable Information (PII) data, etc. All the ancillary systems used for accessing/communicating with critical systems either for operations or maintenance shall also be classified as critical system. The Board/Partners/Proprietor of the Stock Brokers / Depository Participants shall approve the list of critical systems.</p>

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)	<p>Stockbrokers/ Depository Participants shall deploy detection and alerting tools. Members shall create process to prevent, contain and respond to a data breach/ data leak.</p> <ul style="list-style-type: none"> • Whether comprehensive Data Leak Policy is in place • Whether Data Leak Policy is approved by the board • Whether Data Leak Policy is implemented • Exception reporting and escalation mechanism is in place. • Whether incidents related to data breaches / data leaks are reported in timely manner to CERTIN, SEBI and NSE.
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 of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018
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)	<p>Stock Brokers / Depository Participants shall carry out periodic Vulnerability Assessment and Penetration Tests (VAPT) which inter-alia include critical assets and infrastructure components like Servers, Networking systems, Security devices, load balancers, other IT systems pertaining to the activities done as Stock Brokers / Depository Participants etc., in order to detect security vulnerabilities in the IT environment and in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks.</p> <p>The scope of the IT environment taken for VAPT should include all critical assets and infrastructure components (not limited to) like Networking systems, Security devices, Servers, Databases, Applications, Systems accessible through WAN, LAN as well as with public IP's, websites, etc. The scope should include (not limited to):</p> <ul style="list-style-type: none"> * VA of Infrastructure-Internal & External * VA of Applications-Internal & External * External Penetration Testing-Infrastructure & Application * Internal Penetration Testing-Infrastructure & Application * WIFI Testing * Network Segmentation * VA & PT of Mobile applications * OS & DB Assessment * VAPT of Cloud implementation and deployments <p>Testing methodology: The VAPT should provide in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks. The testing methodology should adapt from the following:</p> <ol style="list-style-type: none"> a. SEBI Circular on Cyber Security and Cyber Resilience framework b. National Critical Information Infrastructure Protection Centre (NCIIPC) c. CERT-In Guidelines d. The National Institute of Standards and Technology ("NIST") Special Publication 800-115 e. Latest ISO27001 f. PCI-DSS standards g. Open Source Security Testing Methodology Manual ("OSSTMM") h. OWASP Testing Guide

3(af)	Stock Brokers / Depository Participants shall conduct VAPT at least once in a financial year. All Stock Brokers / Depository Participants are required to engage only CERT-In empaneled organizations for conducting VAPT. The final report on said VAPT shall be submitted to the Stock Exchanges / Depositories after approval from Technology Committee of respective Stock Brokers / Depository Participants, within 1 month of completion of VAPT activity.
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)	Any gaps/vulnerabilities detected shall be remedied on immediate basis and compliance of closure of findings identified during VAPT Post closure confirmation from Auditors shall be submitted to the Stock Exchanges / Depositories within 3 months post the submission of final VAPT report
3(ai)	In addition, Stock Brokers / Depository Participants shall perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system which is a critical system or part of an existing critical system.
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)	All Cyber-attacks, threats, cyber-incidents and breaches experienced by Stock Brokers / Depositories Participants shall be reported to Stock Exchanges / Depositories & SEBI within 6 hours of noticing / detecting such incidents or being brought to notice about such incidents. This information shall be shared to SEBI through the dedicated e-mail id: sbdp-cyberincidents@sebi.gov.in.
6(b)	The incident shall also be reported to Indian Computer Emergency Response team (CERT-In) in accordance with the guidelines / directions issued by CERT-In within 6 hours of noticing such incidents or being brought to notice about such incidents from time to time. The incidents shall be reported to CERT-In via email (incident@cert-in.org.in), Phone (1800-11-4949) and Fax (1800-11-6969). The details regarding methods and formats of reporting cyber security incidents is also published on the website of CERT-In www.cert-in.org.in and will be updated from time to time. Additionally, the Stock Brokers / Depository Participants, whose systems have been identified as “Protected system” by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC.
6(c)	The quarterly reports containing information on cyber-attacks, threats, cyber-incidents and breaches 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 / Exchanges / Depositories and SEBI, shall be submitted to Stock Exchanges / Depositories within 15 days from the quarter ended June, September, December and March of every year.
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)	Cyber Security Advisory – Standard Operating Procedure (SOP) for handling cyber security incidents of intermediaries-as per SEBI directives. The aspects which shall form part of the SOP and whether stock-broker has to complied.
9(b)	Members shall have a well-documented Cyber Security incident handling process document (Standard Operating Procedure - SOP) in place. Such policy shall be approved by Board of the Member (in case of corporate trading member), Partners (in case of partnership firms) or Proprietor (in case of sole proprietorship firm) as the case may be and shall be reviewed annually by the “Internal Technology Committee” as constituted under SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 for review of Security and Cyber Resilience policy.
9(c)	Members shall examine the Cyber Security incident and classify the Cyber Security incidents into High/ Medium/ Low as per their Cyber Security incident handling process document. The Cyber Security incident handling process document shall define decision on Action/ Response for the Cyber Security incident based on severity.
9(d)	Members shall report the Cyber Security incident to Indian Computer Emergency Response Team (CERT-In).
9(e)	Members shall provide the reference details of the reported Cyber Security incident with CERT-In to the Exchange and SEBI. Members shall also provide details, regarding whether CERT-In team is in touch with the Member for any assistance on the reported Cyber Security incident. If the Cyber Security incident is not reported to CERT-In, members shall submit the reasons for the same to the Exchange and SEBI. Members shall communicate with CERT-In/ Ministry of Home Affairs (MHA)/ Cyber Security Cell of Police for further assistance on the reported Cyber Security incident.

9(f)	Members shall submit details whether Cyber Security incident has been registered as a complaint with law enforcement agencies such as Police or its Cyber Security cell. If yes, details need to be provided to Exchange and SEBI. If no, then the reason for not registering complaint shall also be provided to Exchange and SEBI.
9(g)	The details of the reported Cyber Security incident and submission to various agencies by the Members shall also be submitted to Division Chiefs (in-charge of divisions at the time of submission) of DOS-MIRSD and CISO of SEBI
9(h)	The Designated Officer of the Member (appointed in terms of para 6 of the aforementioned SEBI Circular dated December 03, 2018) shall continue to report any unusual activities and events within 6 hours of receipt of such Information as well as submit the quarterly report on the cyber-attacks & threats within 15 days after the end of the respective quarter in the manner as specified in Exchange circular.
10	SECURITY OPERATION CENTER (SOC)
10(a)	Whether organization has set-up Security Operations Center (In-house / Market SOC / Outsourced)
11	TECHNICAL GLITCH
11(a)	Member has reported all instances of technical glitches within the prescribed timelines during the audit period in accordance with NSE circular NSE/COMP/50610 dated December 15, 2021. Member has correctly reported the issues faced and duration of the downtime. Member has implemented all the measures as mentioned in RCAs and has taken necessary steps to prevent the recurrence of such technical glitch