CIRCULAR

Circular No.	20250528-1	Circular Date	20250528
Category	Regulatory and Compliance	Segment	ALL
Subject	Submission of Half Yearly System Audit Report for the period ended March 31, 2025		
Attachments	• Annexures		

Circular Ref. No. 20250528-1 **May 28, 2025**

Subject – Submission of Half Yearly System Audit Report for the period ended March 31, 2025

Members' attention is drawn to SEBI circular no. CIR/MRD/DMS/34/2013 dated November 6, 2013, on the Annual System Audit of Broker Dealers.

Accordingly, members are required to carry out system audit of their trading facility for the period ended March 31, 2025, as per the applicability criteria given below:

Sr No.	Particulars	Broker Type	Terms of Reference (ToR)	Presence of broker	Periodicity of submission of report
1	IML / IBT / DMA / STWT / SOR users and who may also be Type I brokers.	II	TOR II	Presence in not more than 10 locations and number of terminals are not more than 50.	Once in two years
				Presence in more than 10 locations or number of terminals are more than 50.	Annually
2	Algo users and who may also be Type II brokers	III	TOR III	Not Applicable	Half yearly

Broker Dealers who are using trading software as provided by the Exchange (BOLTPLUS ON WEB) and/or software provided by Exchange owned Application Service Provider (ASP) shall not be covered in the system audit.

Timelines for submission of System Audit Report is as given below:

S. No.	Particulars	Due Date for submission to the Exchange
1.	System Audit Report	June 30, 2025
2.	Corrective Action Report	September 30, 2025
3.	Follow on Report	December 31, 2025

Exchange has identified the broker type and periodicity regarding submission of the system audit report based on available data / information and displayed the same in the IIEFS.

Members may note that the above-mentioned reports are required to be submitted only in electronic form through IIEFS (INDIA INX Electronic Filing System). Once IIEFS is activated for submission, submission of System Audit Report shall be considered complete only after Member submits the report to the Exchange and receives an acknowledgment email. Saved reports/reports submitted by auditor will not be considered as final submission.

Kindly note that in case of non/late submission of reports for period ended March 31, 2025, beyond June 30, 2025, disciplinary action/charges will be levied as follows:

A. A charge of USD 2/- per day will be levied from the month of July 2025.
B. Non-Submission within 3 months from the end of due date for submission; the Exchange will withdraw ETI facility for non-submission of systems audit report.

In case of any further clarification, Members may contact on the following:

Name of Department	Tel No.	Email
Membership	079-61993135/3130	inxmembership.ops@indiainx.com

For and on behalf of,
India International Exchange (IFSC) Ltd.

Jay Soni
Manager - Regulatory

System Audit Report User Manual

Table of Contents

1 INTRODUCTION

System Audit Report (SAR) is a module which has been deployed with already existing application – India INX Electronic Filing System (IIeFS) web based application. It is a compliance process as set by the Exchange to enable trading members to submit SAR & other related documents in electronic format.

1.1 SYSTEM OVERVIEW

Name of Process : System Audit Report

Application : India INX Electronic Filing System

Operational Status : Operational

1.2 ACRONYMS & ABBREVIATIONS

A cronyms & Abbreviations	
IIEFS	India INX Electronic Filing System
SAR	System Audit Report
TOR	Terms Of Reference
ESR	Executive Summary Report
CAR	Corrective Action Report
FOR	Follow on Report

1.3 AUTHORIZED USER PERMISSION

The trading members are authorized to use this application to upload their documents related to system audit report to India International Exchange (IFSC) Ltd.

2 PROCESS DETAIL

This is a process to submit System Audit Report and other documents which will be submitted by trading members to Exchange on annual or half yearly basis depending on the member type. **Getting Started**

Members are required to upload all documents in PDF FORMAT only.

The members who are uploading the System audit report in PDF format should scan and upload any one of the Annexure I or II or III depending on the broker type and Annexure IV (Executive summary sheet), Annexure V (Corrective action report) and Annexure VI (Follow on report) along with stamp and sign of the auditor at the end of the report.

Following are the file naming conventions for uploading the required files.

Name of Document	Naming convention of file	Example
Terms Of Reference	MemberID_TOR(TYPE)_MAR18.PDF	1_TORII_MAR18(Example in case TOR II is applicable)
Executive Summary Report	MemberID_ESR_MAR18.PDF	1_ESR_MAR18
Corrective Action Report	MemberID_CAR_MAR18.PDF	1_CAR_MAR18
Follow on Report	MemberID_FOR_MAR18.PDF	1_FOR_MAR18

3 GETTING STARTED

3.1 LOG IN

Member will login in IIeFS with his user ID and password. System will block login ID if user enters wrong password three times.

System Menu

After successful login system will open home page with member details and menu is available on the left hand side.

Following information will be displayed:

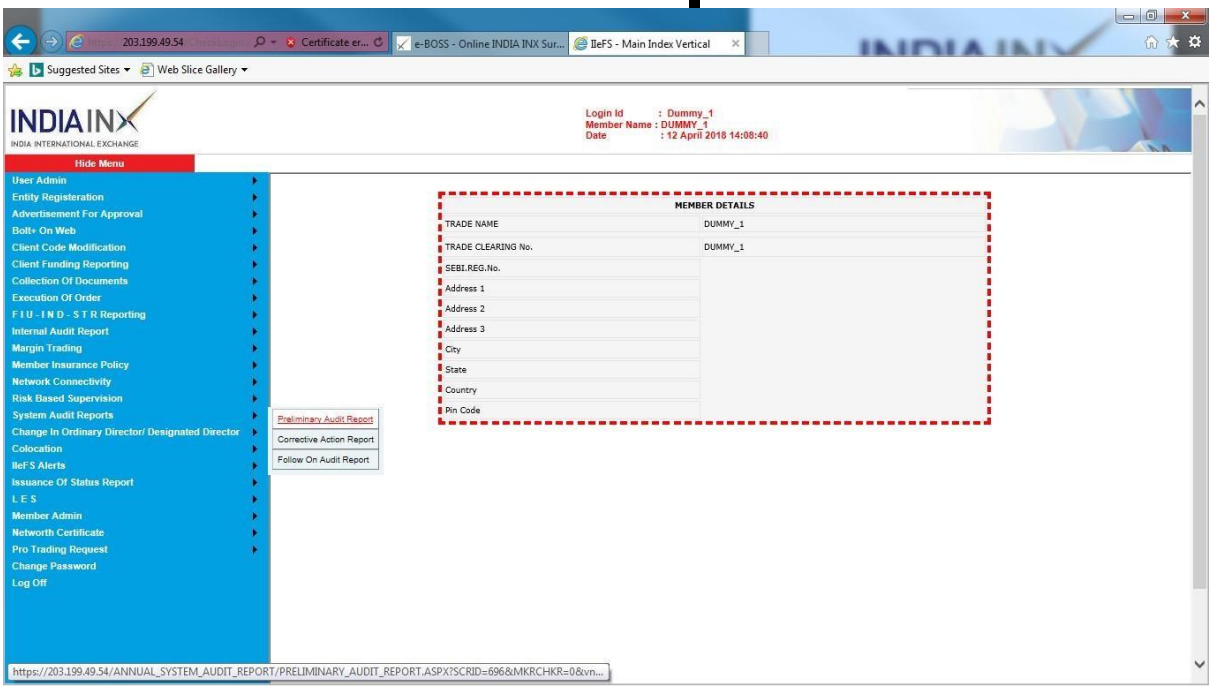
i) Broker type ii) TOR applicable

iii)Periodicity of submission

3.2 PRELIMINARY AUDIT REPORTING

Click on the System Audit report option from the menu and select Preliminary Audit Report Path:

System Audit Report -> Preliminary Audit Report.



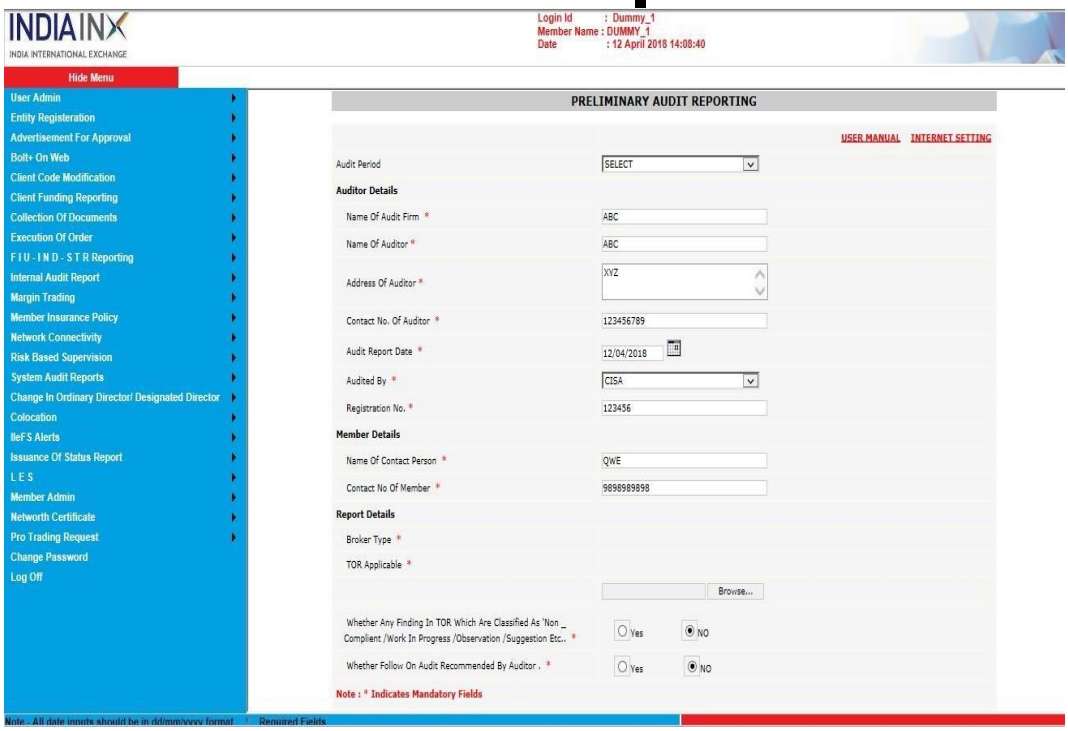
System will navigate on a reporting screen where broker is allowed to enter details about "Preliminary Audit Report".

PROCESS TO UPLOAD SYSTEM AUDIT REPORT (SAR)

These are the following steps to upload system audit report and others documents - **STEP -1**

After selection of preliminary report, system opens a page where member is required to fill following data

- Auditor Information
  Here member will fill information related to Auditor firm.
- Member's Information
  Here member will fill information related to concerned person who is responsible to attend Exchange's query.
- Report Details
  In this block, member is required to upload the required TOR file in pdf format. Naming convention is **MemberID_TOR(TYPE)_MAR15.PDF.**



NOTE:

(1) * Marked field are mandatory.

(2) You can enter date in DD/MM/YYYY format or select from calendar.

(3) If you select wrong date and you want to change date, first you have to delete date then enter new date.

STEP-2

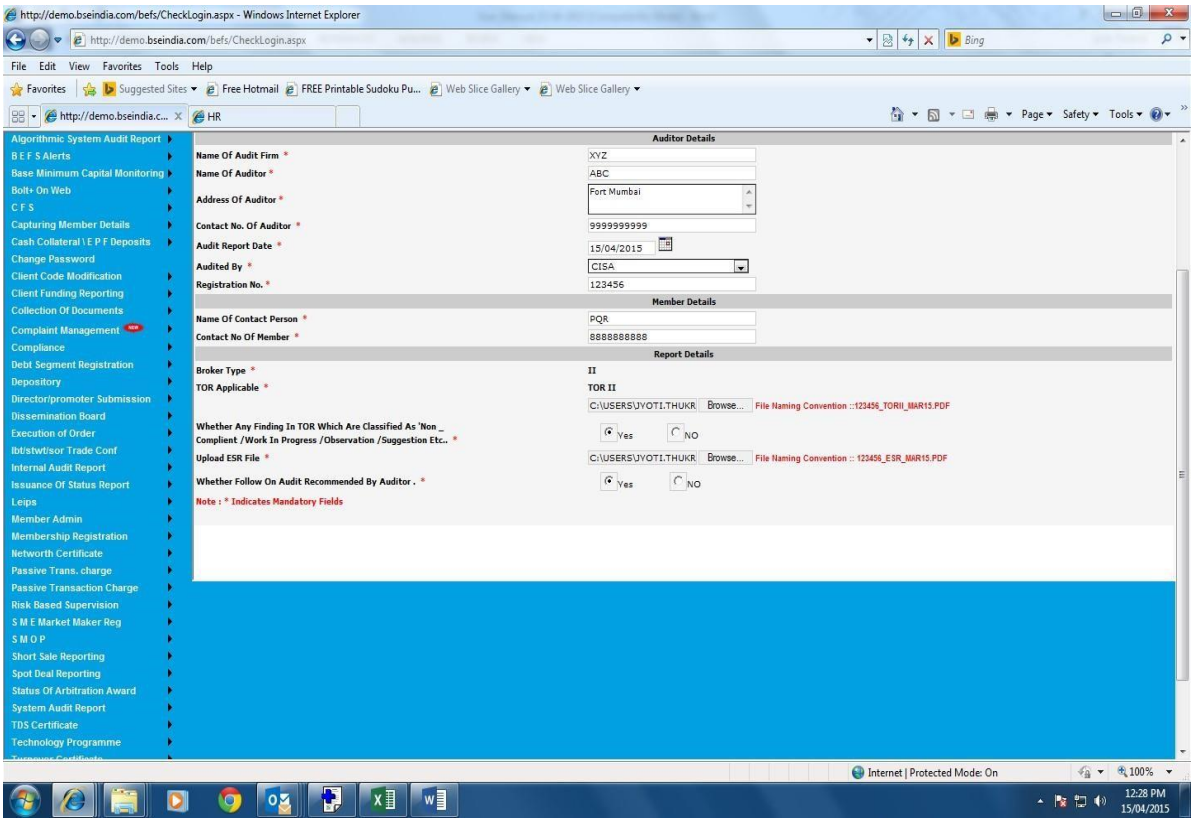
After entering values in all mandatory fields, member is supposed to click on 

button to save entered data of first page. System will populate a message –

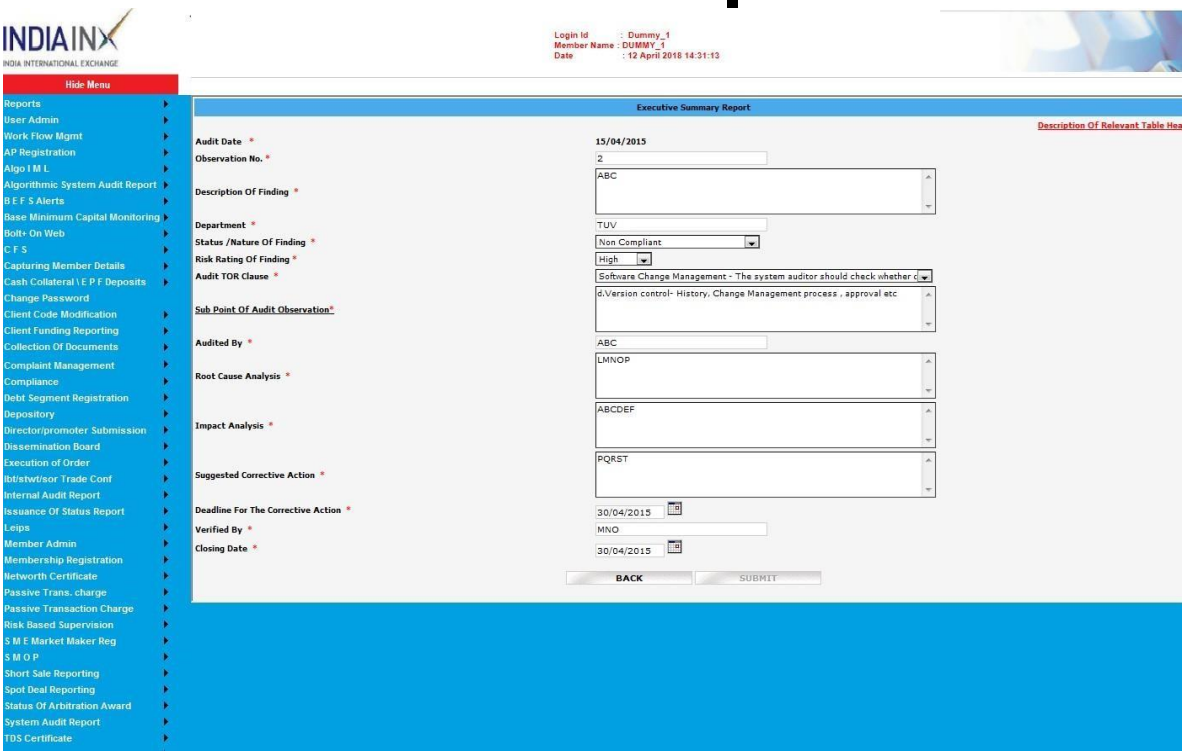
If there are no findings in the report as Non compliance/work in progress/observations or suggestions in the TOR uploaded, Member can directly go to step 6, otherwise go to step 3.

STEP-3

If any observation is identified as Non compliance/work in progress/observations or suggestions, then click on the "Executive Summary Report" link at the bottom of the page.



"Executive Summary Report" is where member is supposed to enter details of findings in TOR. In this screen, all fields are mandatory.

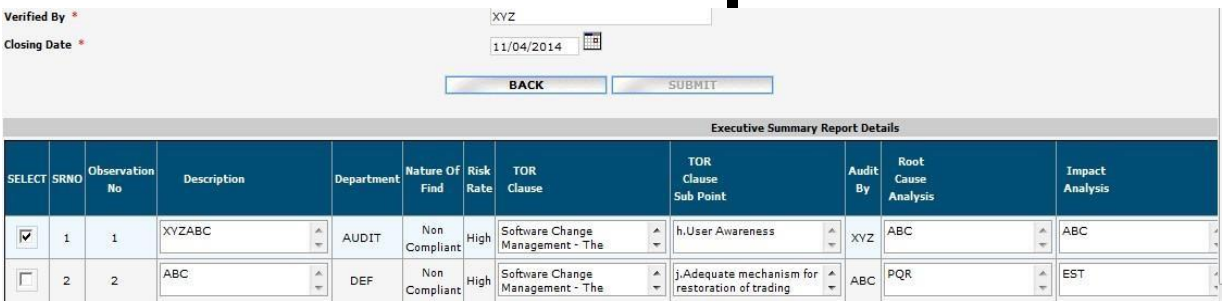


STEP-4

After entering findings, Again member will click on 

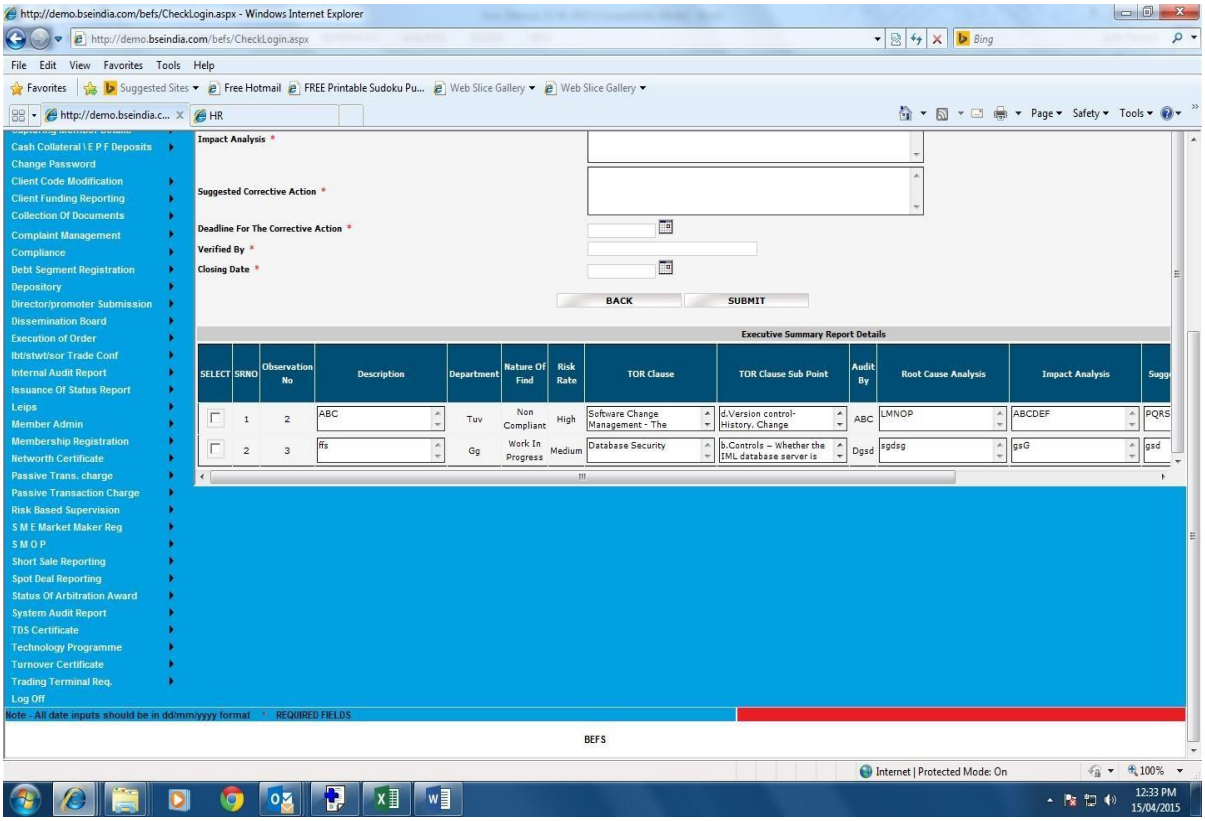
button to save entered data of "Executive Summary Sheet" page.

Following table appears showing the entered details which can be modified by selecting the checkbox.



STEP-5

Once all the findings are updated, member can submit the "Executive Summary Report" by clicking on submit option.



NOTE: After submitting the form no further changes are allowed.

STEP-6

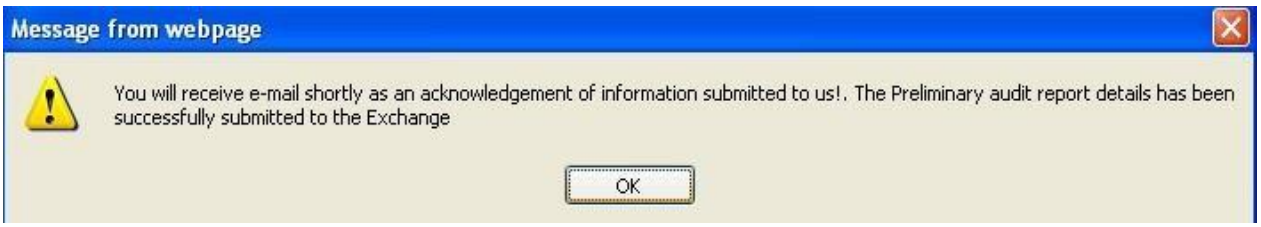
Member will click on SUBMIT button 

to submit preliminary report to exchange.

Following message pops up.

If member will click on 

, system will populate below given message -



Process will complete after clicking on 

.

Note: After submitting the form, the member is not allowed to save any modifications. If tried to do so following message pops up. So care should be taken to check the form before submitting.

3.3 CORRECTIVE ACTION REPORT

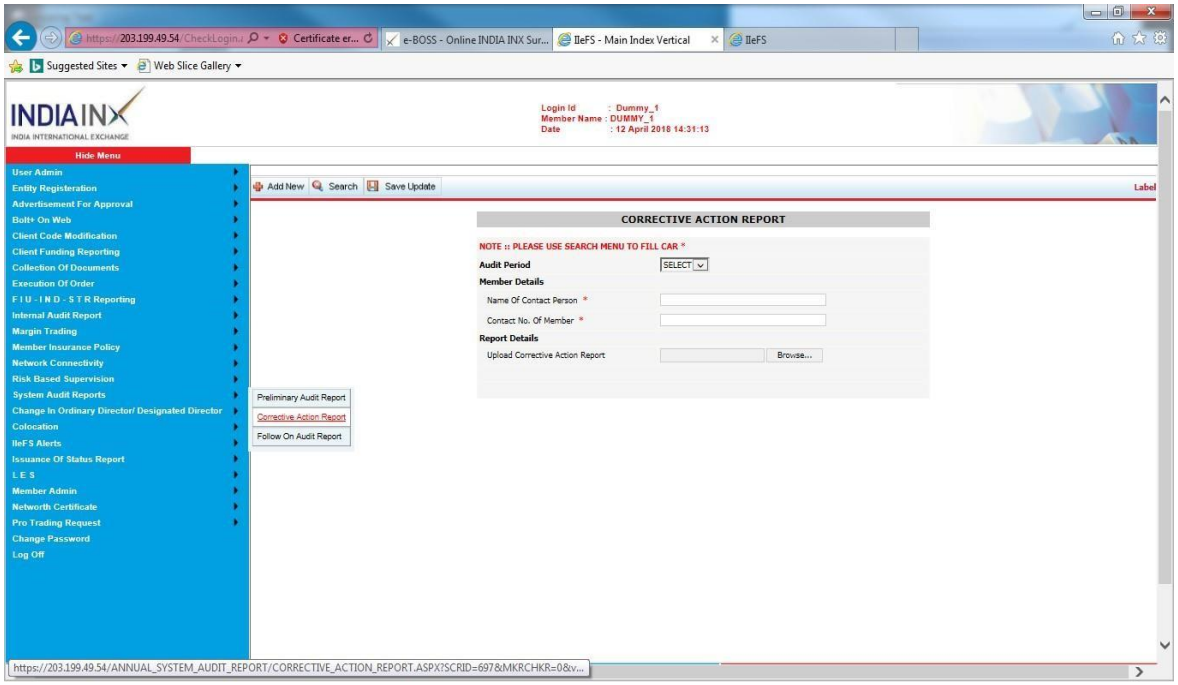
After the Preliminary Audit Report is uploaded the member can upload the Corrective Action Report (if applicable) through Search option. Open home page where menu is available. To open the Corrective Action Report page

Click on **System Audit Report -> Corrective Action Report**

System will navigate on an intermediate screen where member can enter the details about the "Corrective Action Report".

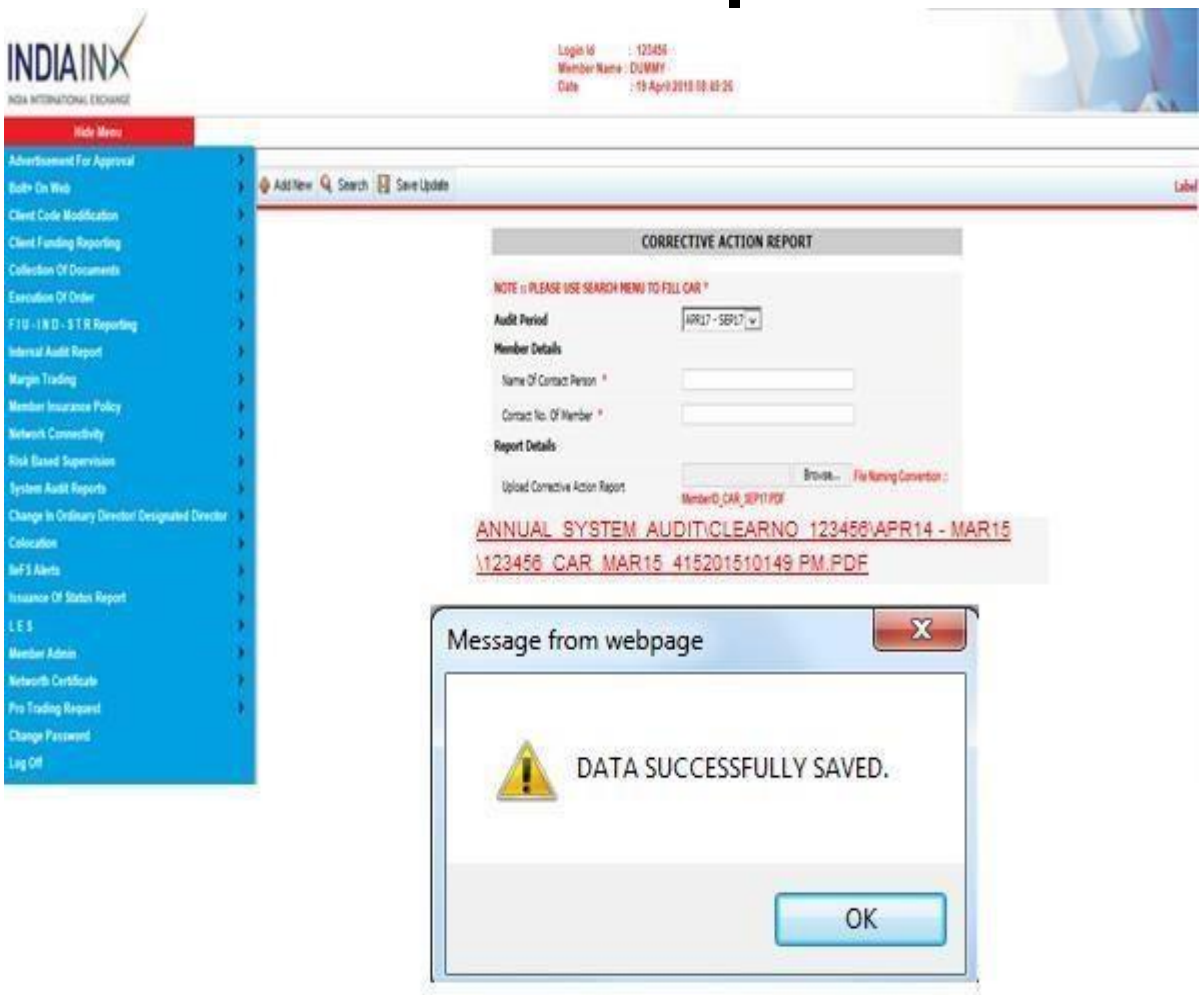
STEP -1

Member should fill in the member details and in report details upload the corrective action report file in pdf format. File Naming Convention: **MemberID_CAR_MAR15**



STEP -2

Click on  button to save entered data of "Corrective Action Report" page. Following message pops up.

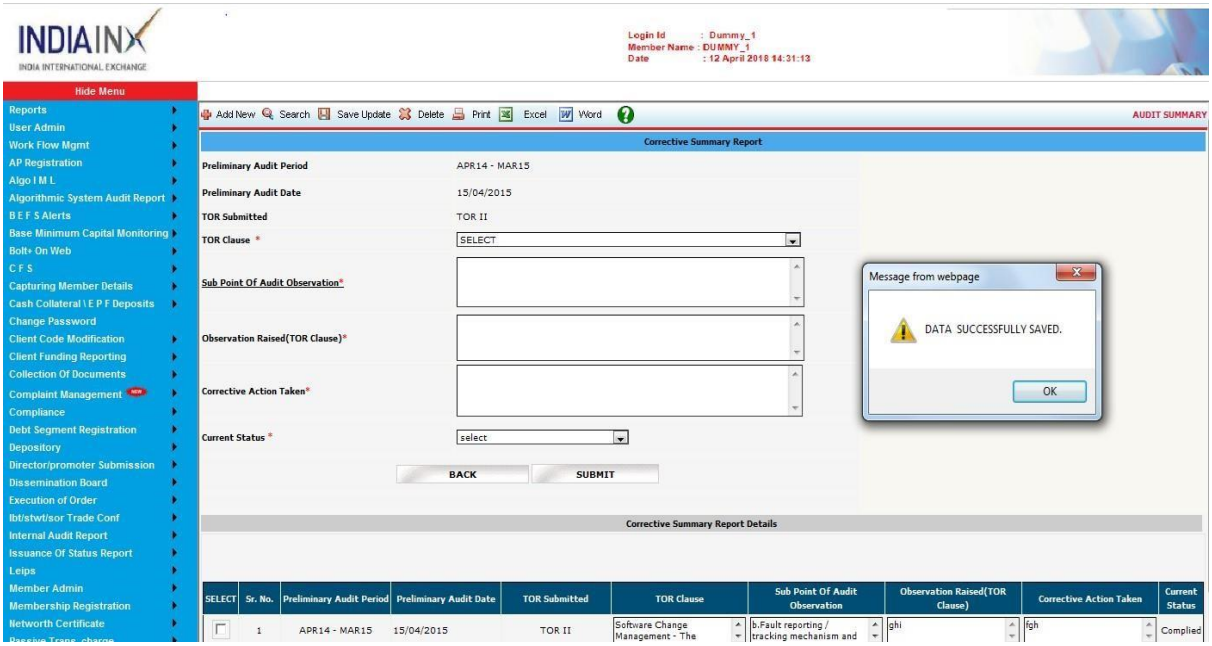

INDIA INX
Hide Menu
Advertisement For Approval
Bolt+ On Web
Client Code Modification
Client Funding Reporting
Collection Of Documents
Execution Of Order
FIU - IND - STR Reporting
Internal Audit Report
Margin Trading
Member Insurance Policy
Network Connectivity
Risk Based Supervision
System Audit Reports
Change In Ordinary Director/ Designated Director
Colocation
IeFS Alerts
Issuance Of Status Report
LES
Member Admin
Networth Certificate
Pro Trading Request
Change Password
Log Off
Add New
Search
Save Update
CORRECTIVE ACTION REPORT
NOTE :: PLEASE USE SEARCH MENU TO FILL CAR !!
Audit Period
APR17 - SEP17
Member Details
Name Of Contact Person *
Contact No. Of Member *
Report Details
Upload Corrective Action Report
Browse...
File Naming Convention :
MemberID_CAR_SEP17.PDF
ANNUAL_SYSTEM_AUDIT\CLEARNO_123456\APR14 - MAR15
\123456_CAR_MAR15_415201510149 PM.PDF
Message from webpage
DATA SUCCESSFULLY SAVED.
OK

STEP -3

After

Click on the OK button, the system will show the "Corrective Summary Report" tab. Click on it to navigate to corrective summary report page. Enter the details and click 

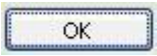
button. Table showing the update will appear at the bottom. Member can select it to modify the details.



STEP-4

Member will click on SUBMIT button 

to submit corrective action report to exchange. Following message pops up.

If member will click on 

, system will populate below given message -

Process will complete after clicking on 

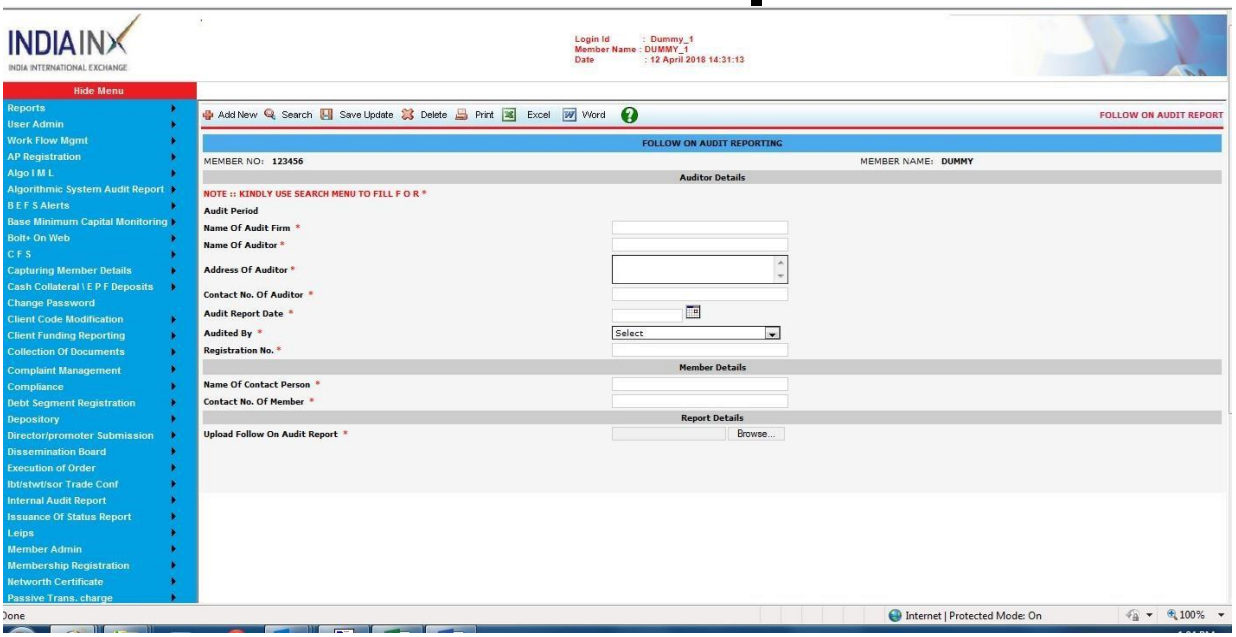
.

Note: After submitting the form, the member is not allowed to save any modifications. If tried to do so following message pops up. So care should be taken to check the form before submitting.

3.4 FOLLOW ON AUDIT REPORT

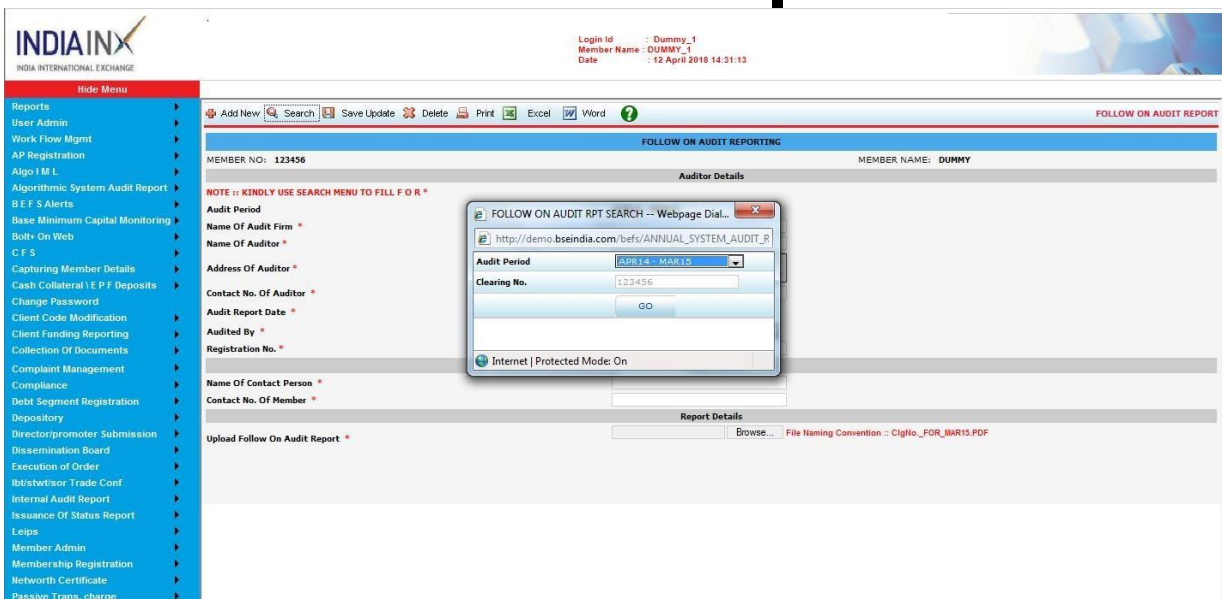
To upload the "Follow on Audit" (if applicable) through Search option, go to Open home page where menu is available. To open the Follow on Audit report page Click on **System Audit Report -> Follow on Audit Report**

System will navigate on an intermediate screen where member can enter the details about the "Follow on Audit Report".



STEP -1

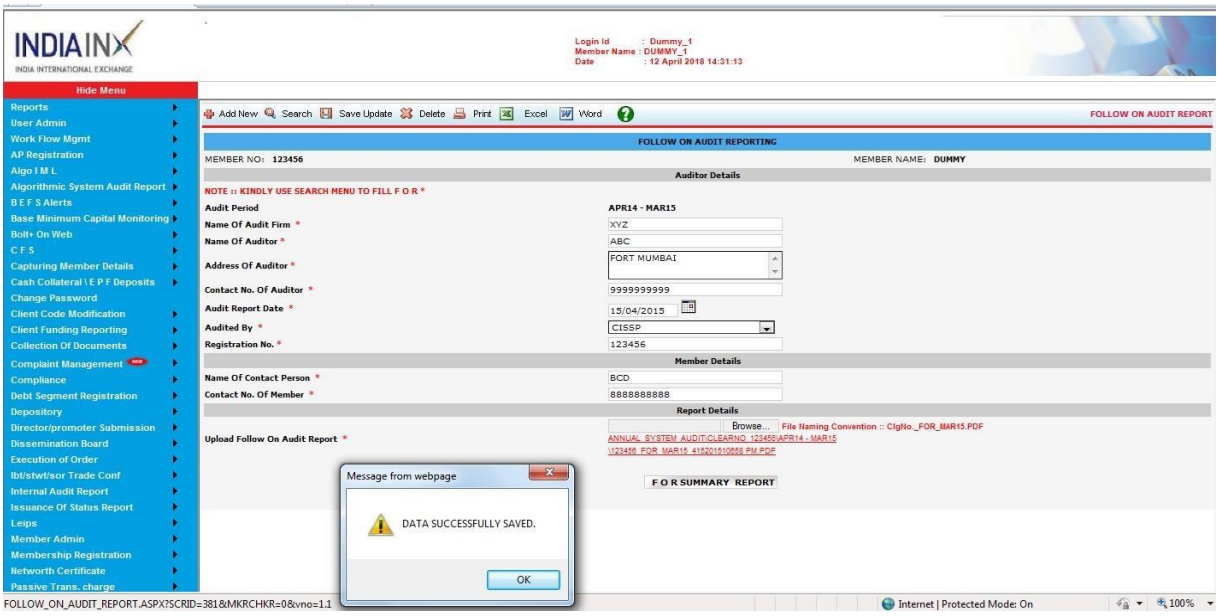
Member should use **Search Menu** for choosing Audit period. After that Member should fill in the Auditor details, member details and report details. Upload the Follow on Audit report in pdf format. File Naming Convention: **MemberID_FOR_MAR14**



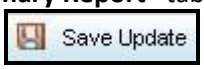
STEP -2

Click on 

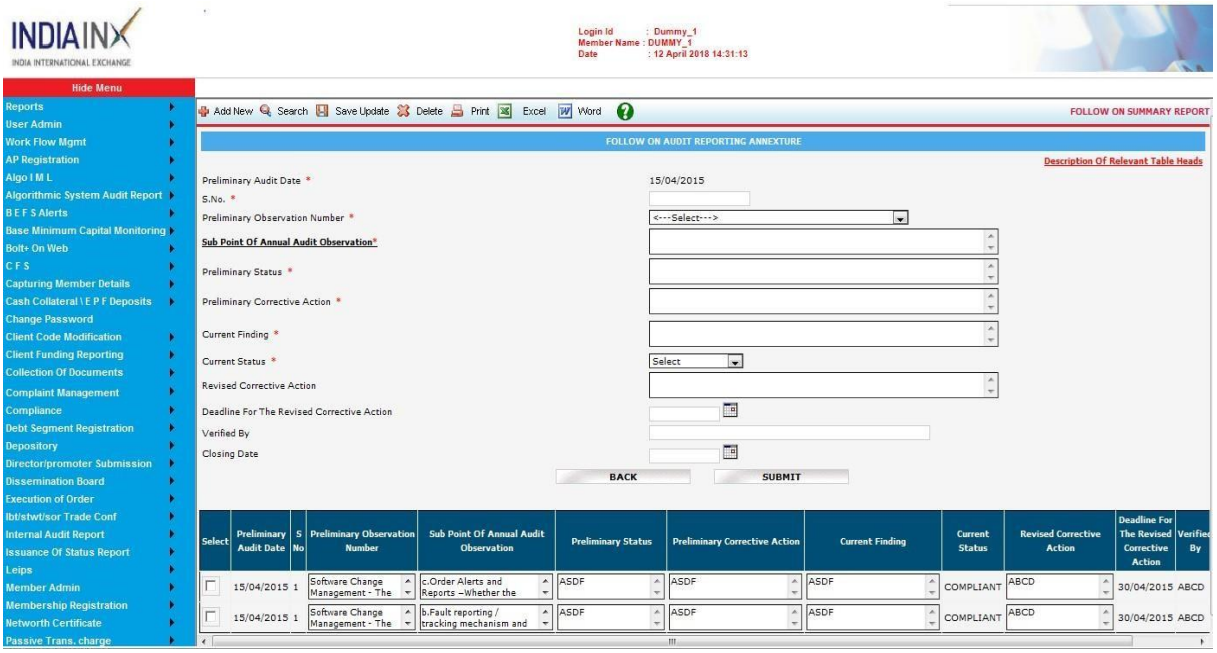
button to save entered data of “Follow on Audit Repor t” page. Following message pops up.



STEP -3

After Click on the OK button, the system will show the "**F O R Summary Report"** tab. Click on it to navigate to FOR summary report page. Enter the details and click 

button. Table showing the update will appear at the bottom. Member can select it to modify the details and save the update.

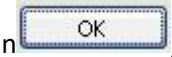


STEP-4

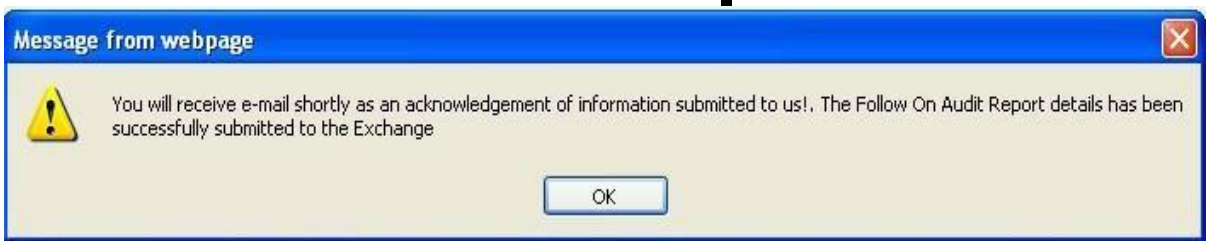
Member will click on SUBMIT button 

to submit FOR summary report to exchange.

Following message pops up.

If member will click on 

, system will populate below given message -



Process will complete after clicking on 

.

Note: After submitting the form, the member is not allowed to save any modifications. If tried to do so following message pops up. So care should be taken to check the form before submitting.

3.5 EXIT FROM SYSTEM

To logoff system, member will click on 

button. If the member is not able to see the Log Off button press F11 to go to full screen mode to see the option at the bottom left corner.

3.6 RESUBMISSION OF REPORT:

Member will be required to resubmit the reports through “Search” option in case the same are rejected by the Exchange due to any reason.

In case member has wrongly uploaded any report and wishes to resubmit the report, kindly mail your request at **inxmembership.ops@indiainx.com or contact 079-61993130/3193.**

Sr no.
1
a
b
c
d
e
f

g
h
i

j
2
a.
b.
c.
d.
e.
f.
g.

h.
i.
j.
3
a.
b.
c.

d.
e.
4
a.
b.

c.
d.
e.

f.
g.
5
a.
b.
c.

d.
6
a.
b.

c.

d.

e.
f.
7
a.
b.
c.

d.

e.

f.
8
a.
b.

c.
d.
e.
f.
g.
h.
i.

j.
k.
l.
m.
9
a.
10
a.

b.
11
a.
b.
c.
d.
e.
f.
g.
h.

i.
j.
k.

l.
m.
n.
o.
p.
q.
r.

s.
t.
12
a.
b.
c.
d.
e.
f.
g.
h.
i.

j.
k.

l.
m.
n.
13
a.
b.
c.
d.
e.

f.
g.
h.
i.
14
a.
b.
15
a.
b.
c.
d.
e.
16
a.
b.
c.

17
a.
b.
c.

d.
e.
f.
g.
h.
i.

j.
k.
18
a.
b.
c.
d.
e.

f.
g.

h.
i.
j.
k.
l.

m.
n.
o.
p.
19
a.
b.
c.
20
a.
21
a.
b.
c.

d.
e.
22
a.
b.
23
a.
b.
c.
d.
e.
f.

g.
h.
i.
j.
k.
l.
m.
n.
o.
p.

I undertake that
guidelines issue

I further confirr

I further confirr

_____

Signature
(Full Name of t

DISA/CISA/CI
Date:
Place:

Annexure I

Terms of Reference (ToR) for Type III Broker

(To be on the letterhead of the system auditor)

System Audit Report for the period _____ to _____)

Particulars
System Control and Capabilities
Order Tracking – The system auditor should verify system process and controls (IBT / DMA / SOR / STWT / ALGO) with regard to order entry, capturing of IP address of order entry terminals, modification / deletion of orders, status of the current order/outstanding orders and trade confirmation.
Order Status/Capture – Whether the system has capability to generate / capture order id, time stamping, order type, scrip details, action, quantity, price and validity etc.
Rejection of orders – Whether system has capability to reject orders which do not go through order level validation at the end of the Member / IBT / DMA / SOR / STWT / ALGO and at the servers of Exchange.
Communication of Trade Confirmation / Order Status – Whether the system has capability to timely communicate to Client regarding the Acceptance/ Rejection of an Order / Trade via various media including e-mail; facility of viewing trade log.
Client ID Verification – Whether the system has capability to recognize only authorized Client Orders and mapping of Specific user Ids to specific predefined location for proprietary orders.
Order type distinguishing capability – Whether system has capability to distinguish the orders originating from IBT/ DMA / STWT/SOR / ALGO. Whether IBT / DMA / SOR / STWT / ALGO orders are having unique flag/ tag as specified by the Exchange and systems identify the orders emanating from IBT / DMA / SOR / STWT / ALGO by populating the 14-digit field in the order structure for every order. Whether Broker is using similar logic/ priorities as used by Exchange to treat IBT / DMA / SOR / STWT/ALGO client orders

The installed system (viz. IBT / DMA / SOR / STWT system) features are as prescribed by the INDIA INX.

Main Features

Price Broadcast

The system has a feature for receipt of price broadcast data

Order Processing: The system has a feature:

- Which allows order entry and confirmation of orders
- Which allows for modification or cancellation of orders placed

Trade Confirmation

- The system has a feature which enables confirmation of trades
- The system has a feature which provides history of trades for the day to the user

The installed system (viz. IBT / DMA / SOR / STWT system) parameters are as per INDIA INX norms

Gateway Parameters

- Trader ID
- IP Address
- Leased Line ID

Execution of Orders / Order Logic

The installed system provides a system based control facility over the order input process

Order Entry

The system has order placement controls that allow only orders matching the system parameters to be placed.

Order Modification

The system allows for modification of orders placed.

Order Cancellation

The system allows for cancellation of orders placed.

Order Outstanding Check

The system has a feature for checking the outstanding orders i.e. the orders that have not yet traded or partially traded.

Trades Information A system based control facility over the trade confirmation process Trade Confirmation and Reporting Feature •Should allow confirmation and reporting of the orders that have resulted in trade •The system has a feature which provides history of trades for the day to the user
Risk Management System (RMS)
Online risk management capability – The system auditor should check whether the system of online risk management (including upfront real-time risk management) is in place for all orders (IBT/ DMA / SOR / STWT / ALGO)
Trading Limits –Whether a system of pre-defined limits / checks such as Single Order Quantity and Single Order Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order value Limit, Order Price limit, Spread order quantity and value limit, Cumulative open order value check (unexecuted orders) are in place and only such orders which are within the parameters specified by the RMS are allowed to be pushed into exchange trading engines. The system auditor should check that no user or branch in the system is having unlimited limits on the above parameters.
Order Alerts and Reports –Whether the system has capability to generate alerts when orders that are placed are above the limits and has capability to generate reports relating to Margin Requirements, payments and delivery obligations.
Order Review –Whether the system has capability to facilitate review of such orders that were not validated by the system.
Back testing for effectiveness of RMS – Whether the system has capability to identify trades which have exceeded the pre-defined limits (Order Quantity and Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order Limit, Order Price limit) and also exceed corresponding margin availability of clients. Whether deviations from such pre-defined limits are captured by the system, documented and corrective steps taken.
Log Management – Whether the system maintains logs of alerts / changes / deletion / activation / deactivation of client codes and logs of changes to the risk management parameters mentioned above. Whether the system allows only authorized users to set the risk parameter in the RMS.
Information Risk Management Has the organization implemented a comprehensive integrated risk assessment, governance and management framework? Are Standards, Guidelines, templates, processes, catalogues, checklists, measurement metrics part of this Framework? Are the risk identification and assessment processes repeated periodically to review existing risks and identify new risks? Has the organization defined procedure/process for Risk Acceptance? Are reports and real time dashboards published in order to report/track Risks?

Order Reconfirmation Facility The installed system provides for reconfirmation of orders which are larger than that as specified by the member's risk management system. The system has a manual override facility for allowing orders that do not fit the system based risk control parameters
Information Risk Management Is there a dedicated Risk Management Team for managing Risk and Compliance activities? Are risks reported to the Senior Management through reports and dashboards on a periodic basis? Is the Risk Management Framework automated? Are SLA's defined for all risk management activities? Has the organization developed detailed risk management program calendar to showcase risk management activities? If yes, is the risk management program calendar reviewed periodically?
Settlement of Trades The installed ystem provides a system based reports on contracts, margin requirements, payment and delivery obligations Margin Reports feature Should allow for the reporting of client wise / user wise margin requirements as well as payment and delivery obligations
Password Security
Organization Access Policy – Whether the organization has a well-documented policy that provides for a password policy as well as access control policy for the API based terminals.
Authentication Capability – Whether the system authenticates user credentials by means of a password before allowing the user to login, and whether there is a system for authentication of orders originating from Internet Protocol by means of two-factor authentication, including Public Key Infrastructure (PKI) based implementation of digital signatures.
Password Best Practices – Whether there is a system provision for masking of password, system prompt to change default password on first login, disablement of user id on entering multiple wrong passwords (as defined in the password policy document), periodic password change mandate and appropriate prompt to user, strong parameters for password, deactivation of dormant user id, etc.

The installed system authentication mechanism is as per the guidelines of the INDIA INX
The installed IBT / DMA / SOR / STWT / ALGO systems use passwords for authentication.
The password policy / standard is documented.
The system requests for identification and new password before login into the system.

The installed system's Password features include
•The Password is masked at the time of entry
•System mandated changing of password when the user logs in for the first time
•Automatic disablement of the user on entering erroneous password on three consecutive occasions
•Automatic expiry of password on expiry of reasonable period of time as determined by member
•System controls to ensure that the password is alphanumeric (preferably with one special character), instead of just being alphabets or just numerical
•System controls to ensure that the changed password cannot be the same as of the last password
•System controls to ensure that the Login id of the user and password should not be the same
•System controls to ensure that the Password should be of reasonable minimum length(and no arbitrary maximum length cap or character class)
•System controls to ensure that the Password is encrypted at members end so that employees of the member cannot view the same at any point of time

Member has implemented the Two Factor Authentication on applications offered to customers through Internet Based Trading (IBT) and Securities Trading through Wireless Technology (STWT).

Session Management

Session Authentication – Whether the system has provision for Confidentiality, Integrity and Availability (CIA) of the session and the data transmitted during the session by means of appropriate user and session authentication mechanisms like SSL etc.

Session Security – Whether there is availability of an end-to-end encryption for all data exchanged between client and broker systems or other means of ensuring session security. Whether session login details are stored on the devices used for IBT and STWT.

Inactive Session – Whether the system allows for automatic trading session logout after a system defined period of inactivity.
Log Management – Whether the system generates and maintain logs of Number of users, activity logs, system logs, Number of active clients.
Cryptographic Controls : Does the organization have a documented process/framework for implementing cryptographic controls in order to protect confidentiality and integrity of sensitive information during transmission and while at rest, using suitable encryption technology? Is the encryption methodology of information involved in business transactions based on Regulation/Law/Standards compliance requirements? Does the organization ensure Session Encryption for internet based applications including the following? Do the systems use SSL or similar session confidentiality protection mechanisms? Do the systems use a secure storage mechanism for storing of usernames and passwords? Do the systems adequately protect the confidentiality of the users' trade data? Does the organization ensure that the data transferred through internet is protected with suitable encryption technologies? Are transactions on the website suitably encrypted?

Cryptographic Controls Is Secret and confidential information sent through e-mails encrypted before sending? Is Secret and confidential data stored in an encrypted format?
Does the organization have deployed data loss prevention (DLP)solutions / processes?
Network Integrity
Seamless connectivity – Whether member has ensured that a backup network link is available in case of primary link failure with the exchange.
Network Architecture – Whether the web server is separate from the Application and Database Server.
Firewall Configuration – Whether appropriate firewall is present between member's trading setup and various communication links to the exchange. Whether the firewall is appropriately configured to ensure maximum security.

Network Security

Are networks segmented into different zones as per security requirements?

Are network segments and internet facing assets protected with Intrusion detection/prevention system (IDS/IPS) and/or Firewall to ensure security?

Has the organization implemented suitable monitoring tools to monitor the traffic within the organization's network and to and from the organizations network?

Does the organization periodically conduct Network Architecture Security assessments in order to identify threats and vulnerabilities?

Are the findings of such assessments tracked and closed?

Are Internet facing servers placed in a DMZ and segregated from other zones by using a firewall?

Is there segregation between application and database servers?

Are specific port/service accesses granted on firewall by following a proper approval process?

Are user and server zones segregated?

Are specific port/service accesses granted on firewall by following a proper approval process?

Are the rules defined in the firewall adequate to prevent unauthorized access to IBT/DMA/STWT

Access Controls

Access to server rooms – Whether adequate controls are in place for access to server rooms and proper audit trails are maintained for the same.

Additional Access controls – Whether the system provides for any authentication/two factor authentication mechanism to access to various components of the terminals (IBT/ DMA / SOR / STWT / ALGO)respectively. Whether additional password requirements are set for critical features of the system. Whether the access control is adequate.

Physical & Environmental Security

Does the organization have a documented process/framework for Physical & Environmental Security?
Are adequate provisions in respect of physical security of the hardware / systems at the hosting location and controls on admission of personnel into the location (audit trail of all entries-exits at location etc.)?
Are security perimeters defined based on the criticality of assets and operations?
Are periodic reviews conducted for the accesses granted to defined perimeters?
Are CCTV cameras deployed for monitoring activities in critical areas?
Is the CCTV footage backed up and can it be made available in case the need arises?
Are suitable controls deployed for combating fire in Data Centre?
Does the organization maintain physical access controls for
•Server Room/Network Room security (environmental controls)
•Server Room .Network Room Security (UPS)
•Server room. network room security (HVAC)
Are records maintained for the access granted to defined perimeters?
Are suitable controls deployed for combating fire in the data centre?

Access Control

Does the organization's documented policy and procedure include the access control policy?
Is access to the information assets based on the user's roles and responsibilities?
Does the system have a password mechanism which restricts access to authenticated users?
Does the system request for identification and new password before login into the system?
Does the system have appropriate authority levels to ensure that the limits can be setup only by persons authorized by the risk / compliance manager?
Does the organization ensure that access control between website hosting servers and internal networks is maintained?

Are records of all accesses requested, approved, granted, terminated and changed maintained?
Are all accesses granted reviewed periodically?

Does the organization ensure that default system credentials are disabled/locked?
Are Application development, Testing (QA and UAT) and Production environments segregated?

Privileged Identity Management Does the organization have a documented process/procedure for defining reviewing and assigning the administrative roles and privileges? Has the organization implemented controls/tools for Privilege Identity Management including at a minimum provisioning, maintenance, monitoring, auditing and reporting all the activities performed by privileged users (Sys Admin, DBA etc.) accessing organization's IT systems? Are Privileges granted to users based on appropriate approvals and in accordance with the user's role and responsibilities? Are all the activities of the privileged users logged? Are log reviews of privileged user logs of admin activity conducted periodically? Is Maker- Checker functionality implemented for all changes by admin? Are records of privileged user provisioning/de-provisioning reviewed?
Extra Authentication Security The systems uses additional authentication measures like smart cards, biometric authentication or tokens etc.
Backup and Recovery
Backup and Recovery Policy – Whether the organization has a well-documented policy on periodic backup of data generated from the broking operations.
Log generation and data consistency - Whether backup logs are maintained and backup data is tested for consistency.
System Redundancy – Whether there are appropriate backups in case of failures of any critical system components.

Backup & Restoration

Does the organization documented policy & procedures include process/policy for Backup and restoration in order to ensure availability of information?

Are backups of the following system generated files maintained as per the INDIA INX guidelines?

At server/gateway level

• Database
• Audit Trails
• Reports

At the user level

• Logs
• History
• Reports
• Audit Trails
• Alert logs
• Market Watch

Does the organization ensure that the user details including user name, unique identification of user, authorization levels for the users activated for algorithm facilities maintained and is available for a minimum period of 5 years?

Does the audit trail capture the record of control parameters, orders, trades and data points emanating from trades executed through algorithm trading?

Does the organization ensure that the audit trail data maintained is available for a minimum period of 5 years?

Does the audit trail for SOR capture the record of orders, trades and data points for the basis of routing decision?

Are backup procedures documented?

Have backups been verified and tested?

Are back up logs maintained?

Are the backup media stored safely in line with the risk involved?

Are there any recovery procedures and have the same been tested?

Are the backups restored and tested periodically to ensure adequacy of backup process and successful restoration?

How will the organization assure customers prompt access to their funds and securities in the event the organization determines it is unable to continue its business in the primary location Network / Communication Link Backup
Is the backup network link adequate in case of failure of the primary link to the BSE?
Is the backup network link adequate in case of failure of the primary link connecting the users?
Is there an alternate communications path between customers and the firm?
Is there e an alternate communications path between the firm and its employees?
• Is there an alternate communications path with critical business constituents, banks and regulators?

How will the organization assure customers prompt access to their funds and securities in the event the organization determines it is unable to continue its business in the primary location System Failure Backup
Are there suitable backups for failure of any of the critical system components like Gateway / Database Server router
Network Switch
Infrastructure breakdown backup
Are there suitable arrangements made for the breakdown in any infrastructure components like Electricity
Water Air Conditioning
Primary Site Unavailability

Have any provision for alternate physical location of employees been made in case of non-availability of the primary site
Disaster Recovery
Are there suitable provisions for Books and records backup and recovery (hard copy and electronic)?
Have all mission-critical systems been identified and provision for backup for such systems been made?

BCP/DR (Only applicable for members having BCP / DR site)

BCP / DR Policy – Whether the member has a well documented BCP/ DR policy and plan? The system auditor should comment on the documented incident response procedures.

The system auditor should comment on the documented incident response procedures which will cover the following:
a. Identification of all critical operations of the Member and also include the process of informing clients in case of any disruptions. While putting in place the BCP/DR plan, members are advised to sufficiently review all potential risks along with its impact on the business.
b. Declaration of incident as a “Disaster” viz. timelines etc. and restoration of operations from DR Site upon declaration of ‘Disaster’ Adequate resources (with appropriate training and experience) should be available at the DR Site to handle all operations during disasters.
c. The declaration of disaster shall be reported in the preliminary report submitted to the Exchange.

Alternate channel of communication – Whether the member has provided its clients with alternate means of communication including channel for communication in case of a disaster. Whether the alternate channel is capable of authenticating the user after asking for additional details or OTP (One-Time-Password).
High Availability – Whether BCP / DR systems and network connectivity provide high availability and have no single point of failure for any critical operations as identified by the BCP/DR policy.
Connectivity with other FMIs – The system auditor should check whether there is an alternative medium to communicate with Stock Exchanges and other FMIs.
Security Incident & Event Management Does the organization have a documented process/policy for Security Incident & Event Management? Does the organization has a documented process/procedure for identifying Security related incidents by monitoring logs generated by various IT assets such as Operating Systems, Databases, Network Devices, etc.? Are all events/incidents detected, classified, investigated and resolved? Are periodic reports published for various identified Security incidents? Does the organization ensure that the logging facilities and the log information Are protected from tampering and unauthorized access?
Security Incident & Event Management Does the organization establish and maintain an incident response team and evaluate incident response plans frequently?
Business Continuity Does the organization have a documented process / framework to ensure the continuation and/or rapid recovery from failure or interruption of business and Information Technology processes and systems? Does the organization maintain a Business Continuity Plan? Does the organization conduct periodic redundancy/ contingency testing? Are BCP drills performed periodically? Is the defined framework/process updated and reviewed periodically?
Does the organization have a Disaster Recovery Site? Does the organization have any documented risk assessments? Does the installations have a Call List for emergencies maintained? Does the organization have robust systems and technical infrastructure in place in order to provide essential facilities, perform systemically critical functions relating to securities market and provide seamless service to their clients?

Does the organisation have distinct primary and disaster recovery sites (DRS) for technology infrastructure, workspace for people and operational processes? Does the organisation have DRS set up sufficiently away (not less than 250 km), from Primary Data Centre (PDC) to ensure that both DRS and PDC are not affected by the same disasters? Have any provision for alternate physical location of employees been made in case of non-availability of the primary site Disaster Recovery? Does the organisation have suitable provisions for Books and records backup and recovery (hard copy and electronic)? Have all mission-critical systems been identified and provision for backup for such systems been made?
Network / Communication Link Backup Controls: (assure customers prompt access to their funds and securities in the event the organization determines it is unable to continue its business in the primary location System Failure Backup Network / Communication Link Backup) 1. Does the organisation have backup network link in case of failure of the primary link to the BSE? 2.Does the organization have adequate backup network link in case of failure of the primary link connecting the users? 3.Does the organization have an alternate communications path between customers and the firm? 4.Does the organization have an alternate communications path between the firm and its employees? 5.Does the organization have an alternate communications path with critical business constituents, banks and regulators? Does the organization have an alternate means of communication including channel for communication for communicating with the clients in case of any disruption. Such communication should be completed within 30 minutes from the time of disruption.
System Failure Backup Controls: (assure customers prompt access to their funds and securities in the event the organization determines it is unable to continue its business in the primary location System Failure Backup) Does the organisation have suitable backups for failure of any of the critical system components like: 1. Gateway / Database Server 2. Router 3. Network Switch 4. Infrastructure breakdown backup
Does the organisation have suitable arrangements made for the breakdown in any infrastructure components like: 1. Electricity 2. Water 3. Air Conditioning 4. Primary Site Unavailability
Segregation of Data and Processing facilities
The system auditor should check and comment on the segregation of data and processing facilities at the member in case the member is also running other business.
Back office data
Data consistency – The system auditor should verify whether aggregate client code data available at the back office of broker matches with the data submitted / available with the stock exchanges through online data view / download provided by exchanges to members.

Trail Logs – The system auditor should specifically comment on the logs of Client Code data to ascertain whether editing or deletion of records have been properly documented and recorded and does not result in any irregularities.
IT Infrastructure Management (including use of various Cloud computing models such as Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS))
IT Governance and Policy – The system auditor should verify whether the relevant IT Infrastructure-related policies and standards exist and are regularly reviewed and updated. Compliance with these policies is periodically assessed.
IT Infrastructure Planning – The system auditor should verify whether the plans/policy for the appropriate management and replacement of aging IT infrastructure components have been documented, approved, and implemented. The activities, schedules and resources needed to achieve objectives related to IT infrastructure have been integrated into business plans and budgets.
IT Infrastructure Availability (SLA Parameters) – The system auditor should verify whether the broking firm has a process in place to define its required availability of the IT infrastructure, and its tolerance to outages. In cases where there is huge reliance on vendors for the provision of IT services to the brokerage firm the system auditor should also verify that the mean time to recovery (MTTR) mentioned in the Service Level Agreement (SLA) by the service provider satisfies the requirements of the broking firm
IT Performance Monitoring (SLA Monitoring) – The system auditor should verify that the results of SLA performance monitoring are documented and are reported to the management of the broker.
Infrastructure High Availability •Does the organization have a documented process for identifying single point of failure? •Does the organization have a documented process for failover? •Does the organization ensure that various components pertaining to networks, servers, storage have sufficient redundancy? •Does the organization conduct periodic redundancy/contingency testing?
Standards & Guidelines Does the organization maintain standards and guidelines for information security related controls, applicable to various IT functions such as System Administration, Database Administration, Network, Application, and Middleware etc.? Does the organization maintain Hardening Standards pertaining to all the technologies deployed within the organization related to Applications, OS, Hardware, Software, Middleware, Database, Network Devices and Desktops? Does the organization have a process for deploying OS, Hardware, Software, Middleware, Database, Network Devices and Desktops after ensuring that they are free from vulnerabilities? Are the defined standards, guidelines updated and reviewed periodically?
Information Security Policy & Procedure Does the organizations documented policy and procedures include the information security policy and if so are they compliant with legal and regulatory requirements? Is the defined policy, Procedure reviewed on a periodic basis?
Information Security Policy & Procedure Are any other standards/guidelines like ISO 27001 etc. being followed? Does the organization have an Information Security Forum to provide overall direction to information security initiatives based on business objectives?

To ensure information security for the Organization in general and the installed system in particular policy and procedures as per the INDIA INX requirements must be established, implemented and maintained

Does the organization's documented policy and procedures include the following policies and if so are they in line with the INDIA INX requirements and whether they have been implemented by the organization?

- Information Security Policy
- Password Policy
- User Management and Access Control Policy
- Network Security Policy
- Application Software Policy
- Change Management Policy
- Backup Policy
- BCP and Response Management Policy
- Audit Trail Policy
- Capacity Management Plan

Does the organization follow any other policy or procedures or documented practices that are relevant?

Are documented practices available for various system processes

- Day Begin
- Day End
- Other system processes
- Audit Trails
- Access Logs
- Transaction Logs
- Backup Logs
- Alert Logs
- Activity Logs
- Retention Period
- Misc.

Is a log of success / failure of the process maintained?

Day Begin
Day End
Other system processes

In case of failure, is there an escalation procedure implemented? •Details of the various response procedures incl. for •Access Control failure •Day Begin failure •Day End failure •Other system Processes failure
Vulnerability Assessment, Penetration Testing & Application Security Assessments: Does the organization have documented processes/procedures for conducting vulnerability assessments, penetration tests and application security assessments? Are these assessments conducted periodically in order to proactively identify threats and vulnerabilities arising from both internal and external sources in order to maintain a strong security posture? **Vulnerability Assessment (VA)** Are periodic vulnerability assessments for all the assets including Servers, OS, Database, Middleware, Network Devices, Firewalls, IDS /IPS etc. conducted? Is Firewall Rule base and IDS/IPS Policy reviews taken up as a part of Vulnerability Assessment? **Penetration Testing (PT)** Are periodic Penetration Tests conducted? Application Security Assessment (AppSec) Are periodic application security assessments conducted? Are reports published for the findings of Vulnerability Assessment/Penetration Testing's/Application Security Assessments? Are findings of Vulnerability Assessment / Penetration Testing's / Application Security Assessments reviewed and tracked to closure?
Information Classification & Protection: Has the organization defined Systematic and documented framework for Information Classification & Protection? Are the information items classified and protected in accordance with business criticality and sensitivity in terms of Confidentiality, Integrity & Availability? Does the organization conduct periodic information classification process audits? Has the organization deployed suitable controls to prevent leakage of sensitive information?
Vulnerability Assessment, Penetration Testing & Application Security Assessments Does the organization maintain an annual VAPT and Application Security Assessment activity calendar? Is periodic Router ACL review conducted as a part of Vulnerability Assessment?
Does the organisation have hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments.
Amazon's AWS S3 and EC2 service Controls: Does the organization check public accessibility of all AWS instances in use. Make sure that no server/bucket is inadvertently leaking data due to inappropriate configurations?
Does the organization ensure proper security of AWS access tokens. The tokens should not be exposed publicly in website source code, any configuration files etc. ?

Does the organisation implement appropriate security measures for testing, staging and backup environments hosted on AWS? Does the organization ensure that production environment is kept properly segregated from these? Does the organisation disable/remove older or testing environments if their usage is no longer required?
The Apache Software Foundation released an emergency patch as part of the 2.15.0 release of Log4j that fixes the Remote Code Execution (RCE) vulnerability. Does the Organizations Application administrators and developers verify the use of Log4j package in their environment and upgrade to version 2.15.0?
Software Change Management - The system auditor should check whether proper procedures have been followed and proper documentation has been maintained for the following:
Processing / approval methodology of new feature request or patches
Fault reporting / tracking mechanism and process for resolution
Testing of new releases / patches / modified software / bug fixes
Version control- History, Change Management process , approval etc.
Development / Test / Production environment segregation.
New release in production – promotion, release note approvals
Production issues / disruptions reported during last year, reasons for such disruptions and corrective actions taken.
User Awareness
The system auditor should check whether critical changes made to the IBT / DMA / STWT/ SOR / ALGO are well documented and communicated to the Stock Exchange.

Change Management

Has the organization implemented a change management process to avoid risks due to unplanned and unauthorized changes for all the information security assets (Hardware, software, networks, applications)?

Does the process at a minimum include the following?

• Planned Changes

Are changes to the installed system made in a planned manner?

Are they made by duly authorized personnel?

• Risk Evaluation Process

Is the risk involved in the implementation of the changes duly factored in?

• Change Approval

Is the implemented change duly approved and process documented?

• Pre-implementation process

Is the change request process documented?

• Change implementation process

Is the change implementation process supervised to ensure system integrity and continuity

• Post implementation process.

Is user acceptance of the change documented?

• Unplanned Changes

In case of unplanned changes, are the same duly authorized and the manner of change documented later?

Patch Management

Does the organization have a documented process/procedure for timely deployment of patches for mitigating identified vulnerabilities?

Does the organization periodically update all assets including Servers, OS, Database, Middleware, Network Devices, Firewalls, IDS /IPS Desktops etc. with latest applicable versions and patches?

SDLC - Application Development & Maintenance Does the organization has any in house developed applications? If Yes, then Does the organization have a documented process/framework to include processes for incorporating, testing and providing sign-off for information risk requirements at various stages of Software Development Life Cycle (SDLC)? Does the SDLC framework incorporate standards, guidelines and procedures for secure coding? Are roles and responsibilities clearly defined for various stakeholders in the SDLC framework? Are Application development, Testing (QA and UAT) and Production environments segregated?
SDLC - Application Development & Maintenance In case of members self-developed system SDLC documentation and procedures if the installed system is developed in-house.
Human Resources Security, Acceptable Usage & Awareness Trainings Are periodic surprise audits and social engineering attacks conducted to assess security awareness of employees and vendors?
Smart order routing (SOR) - The system auditor should check whether proper procedures have been followed and proper documentation has been maintained for the following:
Best Execution Policy – System adheres to the Best Execution Policy while routing the orders to the exchange.
Destination Neutral – The system routes orders to the recognized stock exchanges in a neutral manner.
Class Neutral – The system provides for SOR for all classes of investors.
Confidentiality - The system does not release orders to venues other than the recognized stock Exchange.
Opt–out – The system provides functionality to the client who has availed of the SOR facility, to specify for individual orders for which the clients do not want to route order using SOR.

Time stamped market information – The system is capable of receiving time stamped market prices from recognized stock Exchanges from which the member is authorized to avail SOR facility.
Audit Trail - Audit trail for SOR should capture order details, trades and data points used as a basis for routing decision.
Server Location - The system auditor should check whether the order routing server is located in GIFT IFSC SEZ.
Alternate Mode - The system auditor should check whether an alternative mode of trading is available in case of failure of SOR Facility
Database Security
Access – Whether the system allows database access only to authorized users / applications.
Controls – Whether the database server is hosted on a secure platform, with Username and password stored in an encrypted form using strong encryption algorithms.
User Management
User Management Policy – The system auditor should check whether the member has a well-documented policy that provides for user management and the user management policy explicitly defines user, database and application Access Matrix.
Access to Authorized users – The system auditor should check whether the system allows access only to the authorized users of the System. Whether there is a proper documentation of the authorized users in the form of User Application approval, copies of User Qualification and other necessary documents.
User Creation / Deletion – The system auditor should check whether new user ids were created / deleted as per guidelines of the exchange and whether the user ids are unique in nature.
User Disablement – The system auditor should check whether non-complaint users are disabled and appropriate logs (such as event log and trade logs of the user) are maintained.
User Management system: Reissue of User Ids: User Ids are reissued as per the INDIA INX guidelines. Locked User Accounts: Users whose accounts are locked are unlocked only after documented unlocking requests are made.
Software Testing Procedures - The system auditor should check whether the member has complied with the guidelines and instructions of SEBI / stock exchanges with regard to testing of software and new patches, including the following:
Test Procedure Review – The system auditor should review and evaluate the procedures for system and software/program testing. The system auditor should also review the adequacy of tests.
Documentation – The system auditor should verify whether the documentation related to testing procedures, test data, and resulting output were adequate and follow the organization's standards.
Test Cases – The system auditor should review the internal test cases and comment upon the adequacy of the same with respect to the requirements of the Stock Exchange and various SEBI circulars.

Algorithmic Trading - The system auditor should check whether proper procedures have been followed and proper documentation has been maintained for the following:

Change Management –Whether any changes (modification/addition) to the approved algos were informed to and approved by stock exchange. The inclusion / removal of different versions of algos should be well documented.

Online Risk Management capability- The ALGO server have capacity to monitor orders / trades routed through algo trading and have online risk management for all orders through Algorithmic trading.

The system has functionality for mandatorily routing of orders generated by algorithm through the automated risk management system and only those orders that are within the parameters specified in the risk management systems are allowed to be released to exchange trading system.

The risk management system has following minimum levels of risk controls functionality and only algorithm orders that are within the parameters specified by the risk management systems are allowed to be placed.

A) Individual Order Level:

•Quantity Limits
•Price Range checks
•Trade price protection checks
•Order Value Checks
(Order should not exceed the limit specified by the Exchange)
•Market price protection (the pre-set percentage of LTP shall necessarily be accompanied by a limit price)
•Spread order Quantity and Value Limit
•Immediate or Cancel Orders are not permitted for Commodity Derivatives
•Market Orders are not permitted for Commodity Derivatives
•All orders generated by Algorithmic trading products adhere to the permissible limit of orders per second, if any, as may be specified by SEBI/Exchange.

B) Client Level:

•Cumulative Open Order Value check
•Automated Execution check
•Net position v/s available margins
•RBI violation checks for FII restricted stocks
•Market-wide Position Limits (MWPL) violation checks
•Position limit checks
•Trading limit checks
•Exposure limit checks at individual client level and at overall level for all clients

The risk management system has the following 4 Model risk controls:

1. Circuit Breaker Check
2. Market Depth Check
3. Last Price Tolerance (LPT) Check
4. Fair Value Check

Risk Parameters Controls – The system should allow only authorized users to set the risk parameter. The System should also maintain a log of all the risk parameter changes made.
Information / Data Feed – The auditor should comment on the various sources of information / data for the algo and on the likely impact (run away /loop situation) of the failure one or more sources to provide timely feed to the algorithm. The system auditor should verify that the algo automatically stops further processing in the absence of data feed.
Check for preventing loop or runaway situations – The system auditor should check whether the brokers have real time monitoring systems to identify and shutdown/stop the algorithms which have not behaved as expected.
Algo / Co-location facility Sub-letting – The system auditor should verify if the algo / co-location facility has not been sub-letted to any other firms to access the exchange platform. The system auditor should verify that member is not using co-location/co-hosting facility in Commodity Derivatives Segment. The system auditor should verify that member is not using Algorithmic trading from Exchange Hosted terminals in Commodity Derivatives Segment.
Audit Trail – The system auditor should check the following areas in audit trail: i. Whether the audit trails can be established using unique identification for all algorithmic orders and comment on the same. ii. Whether the broker maintains logs of all trading activities. iii. Whether the records of control parameters, orders, traders and data emanating from trades executed through algorithmic trading are preserved/ maintained by the member. iv. Whether changes to the control parameters have been made by authorized users as per the Access Matrix. The system auditor should specifically comment on the reasons and frequency for changing of such control parameters. Further, the system auditor should also comment on the possibility of such tweaking leading to run away/loop situation. v. Whether the system captures the IP address from where the algo orders are originating.
Systems and Procedures – The system auditor should check and comment on the procedures, systems and technical capabilities of member for carrying out trading through use of Algorithms .The system auditor should also identify any misuse or unauthorized access to algorithms or the system which runs these algorithms Whether installed systems & procedures are adequate to handle algorithm orders/ trades? The system auditor should also identify any misuse or unauthorized access to algorithms or the system which runs these algorithms. Whether details of users activated for algorithm facilities is maintained along with user name, unique identification of user, authorization levels. Does the organization follow any other policy or procedures or documented practices that are relevant?

Reporting to Stock Exchanges – The system auditor should check whether the member is informing the stock exchange regarding any incidents where the algos have not behaved as expected. The system auditor should also comment upon the time taken by the member to inform the stock exchanges regarding such incidents.
Mock Testing: Have all user-ids approved for Algo trading, irrespective of the algorithm having undergone change or not, participated in the mock trading sessions minimum once a month / Participated in the Simulated Environment at least on one trading day during each calendar month.
Additional Points
Vendor Certified Network diagram Date of submission of network diagram to INDIA INX (Only in case of change in network setup, member needs to submit revised scanned copy network diagram along with this report) Verify number of nodes in diagram with actual Verify location(s) of nodes in the network
Antivirus Management Does the organization have a documented process/procedure for Antivirus Management? Are all information assets protected with anti-virus software and the latest anti-virus signature updates? Does the organization periodically performs scans for virus/malicious code on computing resources, email, internet and other traffic at the Network Gateway/entry points in the IT Infrastructure? Does the organization have a documented process/procedure for tracking, reporting and responding to virus related incidents?
Anti-virus Is a malicious code protection system implemented? If Yes, then •Are the definition files up-to-date? •Any instances of infection? •Last date of virus check of entire system
Asset Management Does the organization have a documented process/framework for managing all the hardware & software assets? Does the organization maintain a centralized asset repository? Are periodic reconciliation audits conducted for all the hardware and software assets to confirm compliance to licensing requirements and asset inventory?
Phishing & Malware Protection **For IBT / STWT** Has the organization implemented controls/ mechanism to identify and respond to phishing attempts on their critical websites? Are the organizations websites monitored for Phishing & Malware attacks? Does the organization have a process for tracking down phishing sites?

Compliance

Does the organization have a documented process/policy implemented to ensure compliance with legal, statutory, regulatory and contractual obligations and avoid compliance breaches?

Does the organization ensure compliance to the following?

•IT Act 2000

•SEBI Requirement

Does the organization maintain an integrated compliance checklist?

Are these defined checklists periodically updated and reviewed to incorporate changes in rules, regulations or compliance requirements?

Whether the order routing servers routing ALGO/IBT/DMA/STWT/SOR orders are located in GIFT IFSC SEZ.

Provide address of the IBT / DMA / SOR / STWT server location (as applicable)

Whether the required details of all the API based user ids created in the server of the trading member, for any purpose (viz. administration, branch administration, mini-administration, surveillance, risk management, trading, view only, testing, etc.) and any changes therein, have been uploaded as per the requirement of the Exchange?

If no, please give details.

Whether all the user ids created in the server of the trading member have been mapped to 14 digit codes on a one-to-one basis and a record of the same is maintained?

If no, please give details.

The system has an internal unique order numbering system.

All orders generated by terminals (IBT/DMA/STWT/SOR/ALGO) are offered to the market for matching and system does not have any order matching function resulting into cross trades.

Whether algorithm orders are having unique flag/ tag as specified by the Exchange. All orders generated from algorithmic system are tagged with a unique identifier – **14th digit of field is populated withvalue as mentioned in indiainx.com/circulars/20190827-2/20190827-2.pdf.**

All orders routed through IBT / STWT / DMA / SOR are routed through electronic / automated Risk Management System of the broker to carry out appropriate validations of all risk parameters before the orders are released to the Exchange.

The system and system records with respect to Risk Controls are maintained as prescribed by the Exchange which are as follows :

DOS

Has the organization implemented strong monitoring, logging, detection and analysis capability to detect and mitigate DOS/DDOS attacks?

Does the organization have a documented process/procedure/policy defining roles and responsibilities and plan of action in order to deal with DOS/DDOS attacks pro-actively and post the incidence?

Does the organization collaborate with ISP's for tackling DOS/DDOS attacks?

DOS

Does the organization periodically conducts mock DOS scenarios to have insight into the preparedness in tackling with DOS/DDOS attacks?

Human Resources Security, Acceptable Usage & Awareness Trainings

Has the organization implemented policy/procedure defining appropriate use of information assets provided to employees and vendors in order to protect these assets from inappropriate use?

Are these policies/procedures periodically updated?

Does the organization perform Background Checks for employees (permanent, temporary) before employment?

Does the organization conduct Information Security Awareness Program through trainings and Quiz for employees and vendors?

Independent Audits

Are periodic independent audits conducted by Third Party / internal Auditors?

Are the audit findings tracked to closure?

Capacity Management

•Does the organization have documented processes/procedures for capacity management for all the IT assets?

•Are installed systems & procedures adequate to handle algorithm orders/trades?

•Is there a capacity plan for growth in place?

Third Party Information Security Management

Does the organization have a documented process/framework for Third Party Vendor Management including at a minimum process and procedure for on-boarding/off-boarding of vendors, checklist for prescribing and assessing compliance, assessment and audit for both onsite & offsite vendors?

Does the organization conducts periodic information security compliance audits/reviews for both onsite and offsite vendors?

Are Risks associated with employing third party vendors addressed and mitigated?

Is the defined process/framework periodically reviewed?

The installed systems provides a system based event logging and system monitoring facility which monitors and logs all activities / events arising from actions taken on the gateway / database server, authorized user terminal and transactions processed for clients or otherwise and the same is not susceptible to manipulation. The installed IBT / DMA / SOR / STWT systems has a provision for On-line surveillance and risk management as per the requirements of INDIA INX and includes •Number of Users Logged in / hooked on to the network incl. privileges of each The installed IBT / DMA / SOR / STWT systems has a provision for off line monitoring and risk management as per the requirements of INDIA INX and includes reports / logs on •Number of Authorized Users •Activity logs •Systems logs •Number of active clients
The system has been installed after complying with the various INDIA INX circulars Copy of Undertaking provided regarding the system as per relevant circulars. Copy of application for approval of Internet Trading, if any. Copy of application for approval of Securities trading using Wireless Technology, if any Copy of application for approval of Direct Market Access, if any. Copy of application / undertaking provided for approval of Smart Order Routing, if any.
Insurance - The insurance policy of the Member covers the additional risk of usage of IBT/STWT/SOR/DMA/ALGO as applicable.
Firewall - Is a firewall implemented? Are the rules defined in the firewall adequate to prevent unauthorized access to IBT/DMA/STWT systems
AI/ML
Are adequate safeguards in place to prevent abnormal behaviour of the AI or ML application / System.
Has Member reported details of AI/ML to Exchange on a quarterly basis in accordance with SEBI circular SEBI/HO/MIRSD/DOS2/CIR/P/2019/10 dated January 04, 2019.
Whether AI / ML systems comply for all above System Audit Checklist points. In case of any observation, please report.
Pre-Trade risk controls:
Whether appropriate pre-trade checks, alerts, and controls are built in systems such that an alert shall be generated if the user places limit order at a price which is away from prevailing market prices
MongoDB and Elasticsearch server Controls:
Does organization adhere to the following practices for securing MongoDB: i. Enable Role-based access control to enforce authentication and require users to identify themselves.
Use TLS/SSL for all incoming and outgoing connections including communication between internal components of MongoDB as well as between applications and MongoDB.
Encrypt the MongoDB data stored in the storage layer and use appropriate file system permissions to restrict access to the data.

Use firewalls to minimize overall exposure and ensure that only traffic from trusted sources can reach the system running MongoDB and that MongoDB can only connect to trusted outputs.
Ensure following practices for securing ELK stack instance: i. Use a reverse proxy software such as nginx or mod_proxy (for Apache HTTP server) to restrict direct access to the ELK components and configure it properly to have Role-based access control. ii. Change the default ports of Elasticsearch, Logstash and Kibana on which connections are made. iii. Use firewalls to restrict connections to the system running the ELK stack.
Internal Policy Controls for Technical Glitch
Does the organization provide internet and wireless technology based trading facility? Does the organisation have internal policy to handle technical glitches ?
Does the policy cover following ? 1.Outline the key systems/departments handling the normal function /operation of the Member and assign responsibilities at business owner and technology owner level. 2.Lay down the processes/steps to be adopted in case of technical glitches along with the timelines and communication with concerned stakeholders including clients. 3.Define the Escalation matrix including reporting of such incident to the Exchange. 4.The response and recovery plan of the Members for the timely restoration of systems affected by technical glitch including the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO). 5. Process of handling client complaints.
Remote Access Controls
Does the organization have proper remote access policy framework incorporating the specific requirements of accessing the enterprise resources are securely located in the data center from home, using internet connection?
For implementation of the concept of trusted machine as end users: Does the organization have categorized the machines as official desktops / laptops and accordingly the same are configured to ensure implementation of solution stack considering the requirements of authorized access?
Does the organizations Official devices have appropriate security measures to ensure that the configuration is not tampered with. Does the organization ensure that internet connectivity provided on all official are not getting used for any purpose other than the use of remote access to data center resources?
Does the organization ensure that If personal devices (BYOD) are allowed for general functions, then appropriate guidelines are issued to indicate positive and negative list of applications that are permitted on such devices?. Further, these devices are subject to periodic audit?
Does the organization implement various measures related to Multi-Factor Authentication (MFA) for verification of user access so as to ensure better data confidentiality and accessibility.? VPN remote access through MFA also needs be implemented.
Does the organization ensure that only trusted machine are permitted to access the data center resources? .Does the organizations Virtual Private Network (VPN) remote login is device specific through the binding of the Media Access Control (MAC) address of the device with the IP address to implement appropriate security control measures?

Organization needs to explore a mechanism for ensuring that the employee using remote access solution is indeed the same person to whom access has been granted and not another employee or unauthorized user. 1. At random intervals takes a picture with the webcam and uploads the same to the Member's server, 2. At random intervals pops up and prompts biometric authentication with a timeout period of a few seconds. If there is a timeout, this is flagged on the Member server as a security event.
A suitable video- recognition method has to be put in place to ensure that only the intended employee uses the device after logging in through remote access. Organization needs to implement short session timeouts for better security.
Does the organization monitors Remote access continuously for any abnormal access and are the appropriate alerts and alarms generated to address this breach before the damage is done?
Does the organization have appropriate risk mitigation mechanisms whenever remote access of data center resources is permitted for service providers?
For on-site monitoring, the Member, Does the organization implement adequate safeguard mechanisms such as cameras, security guards, nearby co- workers to reinforce technological activities?
Does the organizations backup, restore and archival functions work seamlessly, particularly if the users have remote access to internal systems.?
Does the organization apply only necessary and applicable pathches to the existing hardware and software?
Does the organization monitor The Security Operations Centre (SOC) engine is periodically monitored and logs are analyzed from a remote location?
Does the organization analyse generated alerts and alarms? And take appropriate decisions to address the security concerns? Are the organizations security controls for the Remote Access requirements integrated with the SOC Engine and part of the overall monitoring of the security posture?
Does the organization have updated the incident response plan in view of the current pandemic? Does the plan cover following : 1.Increase awareness of information technology support mechanisms for employees who work remotely. 2.Implement cyber security advisories received from SEBI, BSE, CERT-IN and NCIIPC on a regular basis. 3.Further, all the guidelines developed and implemented during pandemic situation shall become SOPs post Covid-19 situation for future preparedness. 4.Disable use of Macros in Microsoft office

Whether follow on audit recommended ?

: I have adhered to and complied with the system audit framework / prerequisites / guidelines of SEBI circular no. CIR/MRD/DMS/34/2013 dated November 6, 2013 on A
ed by SEBI / Exchange.

n that I do not have any conflict of interest in conducting fair, objective and independent audit of the Broker Dealer. Further, the directors / partners of my Audit firm are

n that all the branches where ETI/IBT / STWT/ DMA/SOR/Algo (Stike off whichever is not applicable) facility is provided, have been audited and consolidated report ha

he Auditor & Auditing firm)

SM/CISSP Registration Number:

Compliant/Non Compliant/Work In progress/Observation/Suggestion/NA	Major/Minor deviations	Remarks/Observations of the auditor	Management comments in case of non/compliance

"Yes" or "No"			

nnual System Audit of Stock Brokers / Trading Members and further notices / clarifications /

not related to the broker dealer including its directors or promoters either directly or indirectly.

s been submitted.

Annexure II

Terms of Reference (ToR) for Type II Broker

(To be on the letterhead of the system auditor)

System Audit Report for the period _____ to _____)

Sr no.	Particulars	Compliant/Non Compliant/Work In progress/Observation/Suggestion/NA	Major/Minor deviations	Remarks/Observations of the auditor	Management comments in case of non/compliance
1	**System Control and Capabilities**				
1(a)	Order Tracking The system auditor should verify system process and controls at API based terminal (IBT / DMA / SOR / STWT / ALGO) and API adaptor servers covering order entry, capturing of IP address of order entry terminals, modification / deletion of orders, status of current order/outstanding orders and trade confirmation				
1(b)	Order Status/ Capture – Whether the system has capability to generate / capture order id, time stamping, order type, scrip details, action, quantity, price and validity etc.				
1(c)	Rejection of orders – Whether system has capability to reject orders which do not go through order level validation at API level (IBT / DMA / SOR / STWT / ALGO) servers and at the servers of respective stock exchanges				
1(d)	Communication of Trade Confirmation / Order Status – Whether the system has capability to timely communicate to Client regarding the Acceptance/ Rejection of an Order / Trade via various media including e-mail; facility of viewing trade log.				
1(e)	Client ID Verification – Whether the system has capability to recognize only authorized Client Orders and mapping of Specific user Ids to specific predefined location for proprietary orders.				
1(f)	Order type distinguishing capability – Whether API Based Terminal / Application generating IBT / DMA / SOR / STWT / ALGO orders are having unique flag/ tag as specified by the Exchange and systems identify the orders emanating from IBT / DMA / SOR / STWT / ALGO by populating the LocationID in the order structure for every order.				
2	**Software Change Management**				

	Software Change Management The system auditor should check whether changes made to API based terminal-application / Infrastructure have been in adherence to procedures based on policies. In addition following are adhered and maintained				
a	Processing / approval methodology of new feature request or patches				
b	Fault reporting / tracking mechanism and process for resolution				
c	Testing of new releases / patches / modified software / bug fixes				
d	Version control- History, Change Management process , approval etc				
e	New release in production – promotion, release note approvals				
f	Production issues / disruptions reported during last year, reasons for such disruptions and corrective actions taken.				
g	Changes undertaken pursuant to a change to the stock Exchange's trading system				
h	Adequate mechanism for restoration of trading systems to production state at the end of testing session so as to ensure integrity of Broker Dealer's trading system				
i	The auditor should check that Broker Dealers are not using software without requisite approval of stock Exchange and there has not been any unauthorized change to the approved software				
j	The system auditor should check whether critical changes made to API based terminals-application are well documented and communicated to the Stock Exchange.				
3	**Risk Management System (RMS)**				
a	**Online risk management capability –** The system auditor should check whether the system of online risk management (including upfront real-time risk management) is in place for all orders placed through API terminals (IBT/ DMA / SOR / STWT / ALGO).				
b	**Trading Limits –**Whether a system of pre-defined limits / checks such as Single Order Quantity and Single Order Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order value Limit, Order Price limit, Spread order quantity and value limit, Cumulative open order value check(unexecuted orders) are in place and only such orders which are within the parameters specified by the RMS are allowed to be pushed into exchange trading engines. The system auditor should check that no user or branch in the system is having unlimited limits on the above parameters.				
c	**Order Alerts and Reports –**Whether the system has capability to generate alerts when orders that are placed are above the limits and has capability to generate reports relating to Margin Requirements, payments and delivery obligations.				

d	**Order Review –**Whether the system has capability to facilitate review of such orders that were not validated by the system.				
e	**Back testing for effectiveness of RMS –** Whether the system has capability to identify trades which have exceeded the pre-defined limits (Order Quantity and Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order Limit, Order Price limit) and also exceed corresponding margin availability of clients. Whether deviations from such predefined limits are captured by the system, documented and corrective steps taken.				
f	**Log Management –** Whether the system maintains logs of alerts / changes / deletion / activation / deactivation of client codes and logs of changes to the risk management parameters mentioned above. Whether the system allows only authorized users to set the risk parameter in the RMS.				
4	**Smart Order Routing**				
	Smart order routing (SOR)-The system auditor should check whether proper procedures have been followed and proper documentation has been maintained for the following				
a.	**Best Execution Policy –** System adheres to the Best Execution Policy while routing the orders to the exchange.				
b.	**Destination Neutral –** The system routes orders to the recognized stock exchanges in a neutral manner				
c.	**Class Neutral –** The system provides for SOR for all classes of investors.				
d.	**Confidentiality** - The system does not release orders to venues other than the recognized stock Exchange.				
e.	**Opt–out –** The system provides functionality to the client who has availed of the SOR facility, to specify for individual orders for which the clients do not want to route order using SOR				
f.	**Time stamped market information** – The system is capable of receiving time stamped market prices from recognized stock Exchanges from which the member is authorized to avail SOR facility.				
g.	**Audit Trail** - Audit trail for SOR should capture order details, trades and data points used as a basis for routing decision.				
h.	**Server Location** - The system auditor should check whether the order routing server is located in India.				
i.	**Alternate Mode** - The system auditor should check whether an alternative mode of trading is available in case of failure of SOR Facility				
5	**Password Security**				
a	**Organization Access Policy –** Whether the organization has a well documented policy that provides for a password policy as well as access control policy for Exchange Provided Terminals and for the API based terminals.				

b	**Authentication Capability** – Whether the system authenticates user credentials by means of a password before allowing the user to login, and whether there is is a system for authentication of orders originating from Internet Protocol by means of two-factor authentication, including Public Key Infrastructure (PKI) based implementation of digital signatures.				
c	**Password Best Practices –** Whether there is a system provision for masking of password, system prompt to change default password on first login, disablement of user id on entering multiple wrong passwords (as defined in the password policy document), periodic password change mandate and appropriate prompt to user, strong parameters for password, deactivation of dormant user id, etc.				
6	**Session Management**				
a	**Session Authentication** – Whether system has provision for Confidentiality, Integrity and Availability (CIA) of the session and the data transmitted during the session by means of appropriate user and session authentication mechanisms like SSL etc.				
b	**Session Security** – Whether there is availability of an end-to-end encryption for all data exchanged between client and broker systems or other means of ensuring session security. Whether session login details are stored on the devices used for IBT and STWT.				
c	**Inactive Session** – Whether the system allows for automatic trading session logout after a system defined period of inactivity.				
d	**Log Management** – Whether the system generates and maintains logs of Number of users, activity logs, system logs, Number of active clients				

e	**Cryptographic Controls :** Does the organization have a documented process/framework for implementing cryptographic controls in order to protect confidentiality and integrity of sensitive information during transmission and while at rest, using suitable encryption technology? Is the encryption methodology of information involved in business transactions based on Regulation/Law/Standards compliance requirements? Does the organization ensure Session Encryption for internet based applications including the following? Do the systems use SSL or similar session confidentiality protection mechanisms? Do the systems use a secure storage mechanism for storing of usernames and passwords? Do the systems adequately protect the confidentiality of the users' trade data? Does the organization ensure that the data transferred through internet is protected with suitable encryption technologies? Are transactions on the website suitably encrypted? Email Encryption Is secret and confidential information sent through email encrypted before sending? IS secret and confidential data stored in an encrypted format?				
7	**Database Security**				
a	**Access** – Whether the system allows API based terminal - database access only to authorized users / applications.				
b	**Controls** – Whether the API based terminal database server is hosted on a secure platform, with Username and password stored in an encrypted form using strong encryption algorithms.				
8	**Network Integrity**				
a.	**Seamless connectivity** – Whether the Broker Dealer has ensured that a backup network link is available in case of primary link failure with the exchange.				
b.	**Network Architecture** – Whether the web server is separate from the Application and Database Server.				
c.	**Firewall Configuration** – Whether appropriate firewall is present between Broker Dealer's trading setup and various communication links to the exchange. Whether the firewall is appropriately configured to ensure maximum security.				

d.	**Network Security** Are networks segmented into different zones as per security requirements? Are network segments and internet facing assets protected with Intrusion detection/prevention system (IDS/IPS) and/or Firewall to ensure security? Has the organization implemented suitable monitoring tools to monitor the traffic within the organization's network and to and from the organizations network? Does the organization periodically conduct Network Architecture Security assessments in order to identify threats and vulnerabilities? Are the findings of such assessments tracked and closed? Are specific port/service accesses granted on firewall by following a proper approval process? Are user and server zones segregated? Are specific port/service accesses granted on firewall by following a proper approval process? Are the rules defined in the firewall adequate to prevent unauthorized access to IBT/DMA/STWT				
9	**Access Controls (Physical and Logical Access Controls)**				
a	**Additional Access controls** – Whether the system provides for Two Factor / Multifactor authentication mechanism to access to various API based terminal / components (IBT/ DMA / SOR / STWT / ALGO). Whether additional password requirements are set for critical features of the system. Whether the access control is adequate				
b	Are access to the information and assets based on the user's roles and responsibilities? Does the system have a password mechanism which restricts access to authenticated users? Does the system request for identification and new password before login into the system? Does the system have appropriate authority levels to ensure that the limits can be setup only by persons authorized by the risk / compliance manager?				

c	Does the organization ensure that access control between website hosting servers and internal networks is maintained? Are records of all accesses requested, approved, granted, terminated and changed maintained? Are all accesses granted reviewed periodically? Does the organization ensure that default system credentials are disabled/locked?				
d	**Physical & Environmental Security** Does the organization have a documented process/framework for Physical & Environmental Security? Are security perimeters defined based on the criticality of assets and operations? Are periodic reviews conducted for the accesses granted to defined perimeters? Are CCTV cameras deployed for monitoring activities in critical areas? Is the CCTV footage backed up and can it be made available in case the need arises? Are suitable controls deployed for combating fire in Data Center? Does the organization maintain physical access controls for critical areas such as (but not limited to) ·Server Room/Network Room security (environmental controls) ·Server Room .Network Room Security (UPS) ·Server room. network room security (HVAC) . Operations Room Are records maintained for the access granted to defined perimeters? Are records – audit trails configured maintained and reviewed for all accesses Are suitable controls deployed for combating fire in the data center?				

e	**Privileged Identity Management** Does the organization have a documented process/procedure for defining reviewing and assigning the administrative roles and privileges? Has the organization implemented controls/tools for Privilege Identity Management including at a minimum provisioning, maintenance, monitoring, auditing and reporting all the activities performed by privileged users (Sys Admin, DBA etc.) accessing organization's IT systems? Are Privileges granted to users based on appropriate approvals and in accordance with the user's role and responsibilities? Are all the activities of the privileged users logged? Are log reviews of privileged user logs of admin activity conducted periodically? Is Maker- Checker functionality implemented for all changes by admin? Are records of privileged user provisioning/de-provisioning reviewed?				
f	Extra Authentication Security The systems uses additional authentication measures like smart cards, biometric authentication or tokens etc.				
10	**User Management**				
a.	**User Management Policy** – The system auditor should check whether the Broker Dealer has a well documented policy that provides for user management and the user management policy explicitly defines user, database and application Access Matrix.				
b.	**Access to Authorized users** – The system auditor should check whether the system allows access only to the authorized users of the API based System. Whether there is a proper documentation of the authorized users in the form of User Application approval, copies of User Qualification and other necessary documents.				
c.	**User Creation / Deletion** – The system auditor should check whether new users ids were created / deleted as per API based system guidelines of the exchange and whether the user ids are unique in nature.				
d.	**User Disablement** – The system auditor should check whether non-complaint users are disabled and appropriate logs (such as event log and trade logs of the user) are maintained.				

e.	**User Management system:** Reissue of User Ids:User Ids are reissued as per the exchange guidelines. Locked User Accounts:Users whose accounts are locked are unlocked only after documented unlocking requests are made.				
11	**Backup and Recovery**				
a.	**Backup and Recovery Policy** – Whether the organization has a well documented policy on periodic backup and restoration of data generated from critical systems including broking operations.				
b.	**Log generation and data consistency -** Whether backup logs are maintained and backup data is tested for consistency.				
c.	**System Redundancy** – Whether there are appropriate backups in case of failures of any critical system components.				
d.	Do the backup and restoration include following Documented backup and restoration procedures Records of verification and testing of backup and restoration Are backup and restoration logs maintained? Backup and Restoration include - System Generated Files – at server / gateway level, database, audit trials, reports User level – logs, history, reports, audit trails, alert logs, market watch User Details – user name, unique identification, authorization levels Trade and trade related data - control parameters, orders, trades, routing decisions, algo trade details. Backup are maintained and available for a minimum period of 5 years				
12	**BCP/DR (Only applicable for Broker Dealer having BCP / DR site)**				
a.	**BCP / DR Policy** – Does the organization have a well documented BCP/ DR policy and plan?				
b.	The system auditor should comment on the documented incident response procedures. which will cover the following: a.Identification of all critical operations of the Member and also include the process of informing clients in case of any disruptions. While putting in place the BCP/DR plan, members are advised to sufficiently review all potential risks along with its impact on the business. b.Declaration of incident as a “Disaster” viz. timelines etc. and restoration of operations from DR Site upon declaration of ‘Disaster’ Adequate resources (with appropriate training and experience) should be available at the DR Site to handle all operations during disasters. c.The declaration of disaster shall be reported in the preliminary report submitted to the Exchange.				

c	Technical Glitch Management Does the organizations policy to handle technical glitches cover following ? 1.Outline the key systems/departments handling the normal function /operation of the Member and assign responsibilities at business owner and technology owner level. 2.Lay down the processes/steps to be adopted in case of technical glitches along with the timelines and communication with concerned stakeholders including clients. 3.Define the Escalation matrix including reporting of such incident to the Exchange. 4.The response and recovery plan of the Members for the timely restoration of systems affected by technical glitch including the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO). 5.Process of handling client complaints.				
d	Does the organization have a documented process / framework to ensure the continuation and/or rapid recovery from failure or interruption of business and Information Technology processes and systems? - Does the organization conduct periodic redundancy/ contingency testing? -Are BCP drills performed periodically? -Is the defined framework/process updated and reviewed periodically?				
e	Does the organization have a Disaster Recovery Site? Does the organization have any documented risk assessments? Does the installations have a Call List for emergencies maintained? Does the organization have robust systems and technical infrastructure in place in order to provide essential facilities, perform systemically critical functions relating to securities market and provide seamless service to their clients?				
f	**Alternate channel of communication** – Whether the Broker Dealer has provided its clients with alternate means of communication including channel for communication in case of a disaster. Whether the alternate channel is capable of authenticating the user after asking for additional details or OTP (One-Time-Password).				

g	**High Availability** – Whether BCP / DR systems and network connectivity provide high availability and have no single point of failure for any critical operations as identified by the BCP/DR policy.				
h	**Connectivity with other FMIs** – The system auditor should check whether there is an alternative medium to communicate with Stock Exchanges and other FMIs.				
i	Network / Communication Link Backup Controls: 1.Does the organisation have backup network link in case of failure of the primary link to the - exchange? - users / customers? -banks, regulators, depositories etc 2.Does the organization have alternate communications path between - exchange? - users / customers? -banks, regulators, depositories etc does such communication links in case of any disruption, will such communication be completed within 30 minutes from the time of disruption.				
j	**Segregation of Data and Processing facilities** – The system auditor should check and comment on the segregation of data and processing facilities at the Broker Dealer in case the Broker Dealer is also running other business				
k	Security Incident & Event Management Does the organization have a documented process/policy for Security Incident & Event Management? Does the organization has a documented process/procedure for identifying Security related incidents by monitoring logs generated by various IT assets such as Operating Systems, Databases, Network Devices, etc.? Are all events/incidents detected, classified, investigated and resolved? Are periodic reports published for various identified Security incidents? Does the organization ensure that the logging facilities and the log information Are protected from tampering and unauthorized access? Does the organization establish and maintain an incident response team and evaluate incident response plans frequently?				

l	System Failure Backup Controls: (assure customers prompt access to their funds and securities in the event the organization determines it is unable to continue its business in the primary location System Failure Backup) Does the organisation have suitable backups for failure of any of the critical system components like: 1.Gateway / Database Server 2.Router 3.Network Switch 4.Infrastructure breakdown backup				
m	Does the organisation have suitable arrangements made for the breakdown in any infrastructure components like: 1.Electricity 2.Water 3.Air Conditioning 4.Primary Site Unavailability				
13	**Segregation**				
	Segregation In addition to policies has the auditor evidenced Segregation in terms of Business - stock broking & Other business of Broker Dealer Data and Processing facilities Development / Test / Production environment Corporate user and Production / server zones Application and Database servers Internet facing servers placed in a DMZ and segregated from other zones Are firewall used to ensure segregation wherever needed.				
14	**Back office data**				
a	**Data consistency** – The system auditor should verify whether aggregate client code data available at the back office of broker matches with the data submitted / available with the stock exchanges through online data view / download provided by exchanges to members.				
b	**Trail Logs** – The system auditor should specifically comment on the logs of Client Code data to ascertain whether editing or deletion of records have been properly documented and recorded and does not result in any irregularities.				
15	**IT Infrastructure Management**				

a.	The system auditor should verify 1- existence of policies and procedures. 2- policies and procedures are based on International Standards, Frameworks, Best Practices, Applicable Indian Regulation and Legislations published by SEBI, IFSCA, INDIA INX etc. 3- Policies and procedures are regularly reviewed and updated. 4- Policies and procedures are implemented and 5- Compliance with policies and related procedures are periodically assessed and findings reported and closures ensured in reasonable period of time.				
b.	Scope of Policies & Procedures should cover 1. People: Employees, Vendor Staff / Outsourced staff etc related to the organization 2. Processes: all related and relevant processes including Beginning of Day; End of Day etc 3. Technologies: including, but not limited to Systems, Networks, Storage, Application, Database, Middleware and various C$_l$oud Computing Models and Offerings Are following domains covered in Poicies and Procedures				

c.	1. IT Management 2. Planning 3. Asset Management 4. Change Management 5. Availability & High Availability Management 6. Capacity and Performance Management 7. Informati on Security (covering various controls) 8. Baseline and Hardening 9. Vulnerability Assessment and Management 10. Penetration Testing 11. Supply Chain, Third Party, Vendor – Outsourcing Management 12. Password Policy 13. User Lifecycle Management 14. Access Control (Logical and Physical Access Control) 15. Network Security 16. Application Software Development, Maintenance and Security 17. Segregation of operating environments 18. Physical and Environmental Security 19. Data and Information Classification and Protection 20. Backup and Restoration 21. Audit Trail and Log Management 22. BCP and Response Management 23. Cloud Computing and Security Management covering a. Agreements b. Hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments. c. Service Controls: d. Public accessibility of all cloud instances in use. e. Cloud Server/ Bucket configurations to prevent Data leakage f. Security / Cryptographic Key rotation				
d.	**IT Infrastructure Planning –** The system auditor should verify whether the plans/policy for the appropriate management and replacement of aging IT infrastructure components have been documented, approved, and implemented. The activities, schedules and resources needed to achieve objectives related to IT infrastructure have been integrated into business plans and budgets.				

e	**IT Infrastructure Availability (SLA Parameters) –** The system auditor should verify whether the broking firm has a process in place to define its required availability of the IT infrastructure, and its tolerance to outages. In cases where there is huge reliance on vendors for the provision of IT services to the brokerage firm the system auditor should also verify that the mean time to recovery (MTTR) mentioned in the Service Level Agreement (SLA) by the service provider satisfies the requirements of the broking firm.				
f.	**IT Performance Monitoring (SLA Monitoring)** – The system auditor should verify that the results of SLA performance monitoring are documented and are reported to the management of the broker.				
g.	**Infrastructure High Availability** ·Does the organization have a documented process for identifying single point of failure? ·Does the organization have a documented process for failover? ·Does the organization ensure that various components pertaining to networks, servers, storage have sufficient redundancy? ·Does the organization conduct periodic redundancy/contingency testing?				
16	**Exchange specific exceptional reports**				
	Exchange specific exceptional reports – The additional checks recommended by a particular exchange need to be looked into and commented upon by the system auditor over and above the ToR of the system audit.				
17	**Software Testing Procedures**				
a	**Software Testing Procedures -** The system auditor shall audit whether the Broker Dealer has complied with the guidelines and instructions of SEBI / stock exchanges with regard to testing of software and new patches including the following:				
b	**Test Procedure Review** – The system auditor should review and evaluate the procedures for system and program testing. The system auditor should also review the adequacy of tests.				
c	**Documentation** – The system auditor should review documented testing procedures, test data, and resulting output to determine if they are comprehensive and if they follow the organization's standards.				
d	**Test Cases** – The system auditor should review the test cases and comment upon the adequacy of the same with respect to the requirements of the Stock Exchange anld various SEBI Circulars.				
e	**Testing of software**: The system auditor should verify whether member has complied with the process for testing of their new/modified software as prescribed by SEBI vide its circular dated August 19, 2013 February 7, 2014 and November 24, 2020 regarding testing in (i) Simulated test environment (ii) Mock testing (iii) User Acceptance testing (UAT)				

18	**Artificial Intelligence/Machine Learning**				
a.	Are adequate safeguards in place to prevent abnormal behaviour of the AI or ML application / System.				
b.	Has Member reported details of AI/ML to Exchange on a quarterly basis in accordance with SEBI circular SEBI/HO/MIRSD/DOS2/CIR/P/2019/10 dated January 04, 2019.				
c.	Whether AI / ML systems comply for all above System Audit Checklist points. In case of any observation, please report.				
19	**Remote Access Controls**				
a	Does the organization have proper remote access policy framework incorporating the specific requirements of accessing the enterprise resources are securely located in the data center from home, using internet connection? For implementation of the concept of trusted machine as end users: Does the organization have categorized the machines as official desktops / laptops and accordingly the same are configured to ensure implementation of solution stack considering the requirements of authorized access? Does the organization ensure that only trusted machine are permitted to access the data center resources? Does the organizations Official devices have appropriate security measures to ensure that the configuration is not tampered with. Does the organization ensure that internet connectivity provided on all official are not getting used for any purpose other than the use of remote access to data center resources?. Does the organization ensure that If personal devices (BYOD) are allowed for general functions, then appropriate guidelines are issued to indicate positive and negative list of applications that are permitted on such devices?. Further, these devices are subject to periodic audit? Does the organization implement various measures related to Multi-Factor Authentication (MFA) for verification of user access so as to ensure better data confidentiality and accessibility.? VPN remote access through MFA also needs be implemented. Does the organizations Virtual Private Network (VPN) remote login is device specific through the binding of the Media Access Control (MAC) address of the device with the IP address to implement appropriate security control measures?. Does the organization have mechanism for ensuring that the employee				
20	**SEBI and Exchange Compliances**				

a	Auditor to list all applicable Circulars, Notices, Guidelines, and advisories published by SEBI and Exchanges related to Cyber Security and Cyber Resilience and mention 1-Adherence to all such Circulars, Notices, Guidelines, and advisories published 2-Reporting adherences based on prescribed periodicity in point 1 above				
21	**System Audit**				
a.	The System Auditor should verify the implementation of a)Recommendations in previous system audit report and b)Action Taken in case of medium / weak areas in reports submitted for prior approval.				
b.	The System auditor should verify the observations / issues / recommendations mentioned in the previous system audit report and cover open items in the report and specify whether the member has implemented those observations / issues / recommendations/ open items. If not, provide the reasons for not implementation .				
c.	The System auditor should verify if member have been rated as "Medium/Weak" in any areas by System auditor during audit period (prior to granting approval for Internet based Trading/ Direct Market Access/ SOR/ Wireless securities trading) please provide action taken by member on these areas .				
d	Comments of the auditor on any other area				
	Whether follow on audit recommended ?	"Yes" or "No"			

I undertake that I have adhered to and complied with the system audit framework / prerequisites / guidelines of SEBI circular no. CIR/MRD/DMS/34/2013 dated November 6, 2013 on Annual System Audit of Stock Brokers / Trading Members and further notices / clarifications / guidelines issued by SEBI / Exchange.

I further confirm that I do not have any conflict of interest in conducting fair, objective and independent audit of the Broker Dealer. Further, the directors / partners of my Audit firm are not related to the Broker Dealer including its directors or promoters either directly or indirectly.

I further confirm that all the branches where ETI/IBT / STWT/ DMA/SOR/Algo (Stike off whichever is not applicable) facility is provided, have been audited and consolidated report has been submitted.

_____

Signature

(Full Name of the Auditor & Auditing firm)

DISA/CISA/CISM/CISSP Registration Number:
Date:
Place:

Annexure III Executive Summary Sheet
(To be on the letterhead of the system auditor)

System Audit Report for the period _____ to _____)

Audit Date	Observation No	Description of Finding	Department	Status / Nature of Findings	Risk Rating of Findings	Audit TOR Clause

I undertake that I have adhered to and complied with the system audit framework / prerequisites /
CIR/MRD/DMS/34/2013 dated November 6, 2013 on Annual System Audit of Stock Brokers / T
/ guidelines issued by SEBI / Exchange.

I further confirm that I do not have any conflict of interest in conducting fair, objective and inde
Further, the directors / partners of my Audit firm are not related to the Broker Dealer including it
indirectly.

I further confirm that all the branches where ETI-IBT / STWT/ DMA facility is provided, have b
been submitted.

_____	
Signature	
(Full Name of the Auditor & Auditing firm)	
DISA/CISA/CISM /CISSP Registration Number:	
Date:	
Place:	

Description of relevant Table heads

1. Audit Date – This indicates the date of conducting the audit.

2. Description of Findings/ Observations – Description of the findings in sufficient detail, refe
procedures, interview notes, screen shots etc.)

3. Status/ Nature of Findings - the category can be specified for example:

a. Non Compliant

b. Work In
progress
c. Observation
d. Suggestion

4. Risk Rating of Findings – A rating has to been given for each of the observations based on tl
as the suggested priority for action.

Rating	**Description**
HIGH	Weakness in control those represent exposure to the organization or risks that could lead to instances of non compliance with the requirements of TORs. These risks need to be addressed with utmost priority.
MEDIUM	Potential weakness in controls, which could develop into an exposure or issues that represent areas of concern and may impact internal controls. These should be addressed reasonably promptly.

LOW	Potential weaknesses in controls, which in combination with other weakness can develop into an exposure. Suggested improvements for situations not immediately/directly affecting controls.

5. Audit TOR Clause – The TOR clause corresponding to this observation
6. Root cause Analysis –A detailed analysis on the cause of the nonconformity
7. Impact Analysis – An analysis of the likely impact on the operations/ activity of the organizat
8. Suggested Corrective Action –The action to be taken by the broker to correct the nonconforn

Audited By	Root Cause Analysis	Impact Analysis	Suggested Corrective Action	Deadline for the Corrective Action	Verified By	Closing Date

/ guidelines of SEBI circular no.
Trading Members and further notices / clarifications

pendent audit of the Broker Dealer.
:s directors or promoters either directly or

een audited and consolidated report has

rencing any accompanying evidence (e.g. copies of

ıeir impact and severity to reflect the risk exposure, as well

tion
nity

Annexure IV (Corrective Action Report)
(To be on the letterhead of the Member)

System Audit Report for the period _____ to _____)

Sr No.	Preliminary Audit period	Preliminary audit date	TOR submitted(I, II or III)	TOR Clause	Observation raised(TOR clause)

Name of Compliance officer/ Designated Director

Signature of Compliance officer/Designated Director

Date

Corrective action taken	Current status(Complied/Non compliant/ work in progress)

AnnexureV(Follow on Report)
(To be on the letterhead of the system auditor)

System Audit Report for the period _____ to _____)

Preliminary audit date	Sr No.	Preliminary observation number	Preliminary status	Preliminary Corrective action	Current Finding	Current Status	Revised Corrective Action	Deadline for the revised corrective action	Verified by	Closing date

I undertake that I have adhered to and complied with the system audit framework / prerequisites / guidelines of SEBI circular no. CIR/MRD/DMS/34/2013 dated November 6, 2013 on Annual System Audit of Stock Brokers / Trading Members and further notices / clarifications / guidelines issued by SEBI / Exchange.

I further confirm that I do not have any conflict of interest in conducting fair, objective and independent audit of the Broker Dealer. Further, the directors / partners of my Audit firm are not related to the Broker Dealer including its directors or promoters either directly or indirectly.

I further confirm that all the branches where ETI/IBT / STWT/ DMA facility is provided, have been audited and consolidated report has been submitted.

_____
Signature

(Full Name of
the Auditor &
Auditing firm)
DISA/CISA/CI
SM/CISSP
Registration
Number:
Date:
Place:

Description of
relevant Table
heads

1. Preliminary Status- The original finding as per preliminary System Audit Report
2. Preliminary Corrective Action- The original corrective action as prescribed in the preliminary System Audit report
3.Current Finding-The current finding w.r.t. the issue
4.Current Status-Current status of the issue viz Compliant, Non compliant
5.Revised Corrective Action-The revised corrective action prescribed w.r.t. the Non Compliant/WIP issues