National Stock Exchange of India Limited

Circular

DEPARTMENT: INSPECTION	
Download Ref No: NSE/INSP/56216	**Date: March 29, 2023**
Circular Ref. No: 27/2023	

To All Trading Members,

Sub: Uniform formats for System Audit and Cyber Security and Cyber Resilience Audit reports across Exchanges

This has reference to the formats for submission of System Audit and Cyber Security and Cyber Resilience Audit reports.

To simplify the submission process and ensure uniform formats across Exchanges, the formats for System Audit and Cyber Security and Cyber Resilience Audit reports submissions have been revised, under the guidance of SEBI and in consultation with other Exchanges. Accordingly, the revised and updated formats of System Audit and Cyber Security and Cyber Resilience Audit reports are attached as **Annexure – A and Annexure – B respectively**.

The updated formats of System Audit and Cyber Security and Cyber Resilience Audit reports submission for the period ended March 31, 2023, along with relevant guidelines and annexures, shall be communicated through a separate circular.

All members are advised to take note of the above to bring the provisions of this circular to the notice of the auditors and put in place adequate systems and procedures to ensure strict adherence to the compliance requirements.

For and on behalf of
National Stock Exchange of India Limited

Ajinkya Nikam
Senior Manager– Inspection

National Stock Exchange of India Limited

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

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

Annexure A

Terms of Reference for System Audit

Section	Sub-section	Area of Verification	Type II	Type III
1		**System Control and Capabilities**		
1	A	Order Tracking – The system auditor should verify system process and controls at API based terminals (CTCL / SOR/ IBT / STWT / ALGO / DMA etc.) 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.	Yes	Yes
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.	Yes	Yes
1	C	Rejection of orders – Whether system has capability to reject orders which do not go through order level validation at the end of the stock broker CTCL / IBT / SOR/ STWT / ALGO / DMA etc.. and at the servers of Exchange.	Yes	Yes
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.	Yes	Yes
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.	Yes	Yes
1	F	Order type distinguishing capability –Whether system has capability to distinguish the orders originating from CTCL / IBT / STWT / ALGO / DMA/SOR etc. Whether CTCL / IBT / STWT / ALGO / DMA / SOR etc. orders are having unique flag/ tag as specified by the Exchange and systems identify the orders emanating from CTCL / IBT / STWT/ALGO/ DMA/SOR etc.. by populating the 15-digit CTCL field in the order structure for every order. Whether Broker is using similar logic/ priorities as used by Exchange to treat CTCL / IBT / WT /DMA /SOR etc. client orders	Yes	Yes

1	G	The installed CTCL system parameters are as per Exchange norms: • Approved CTCL / IBT / STWT / ALGO / DMA / SOR etc.. Software Name and Version No (as applicable) and • Strategy Name & Version No. • Software developed by • Order Gateway Version • Risk Administration / Manager Version • Front End / Order Placement Version Provide address of the CTCL / IBT / DMA / SOR / STWT/ ALGO server location (as applicable).	Yes	Yes
1	H	The installed system (viz. CTCL/ IBT / STWT / SOR / DMA/SOR system) features are as prescribed by the Exchange. 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	Yes	Yes
1	I	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.	Yes	Yes

1	J	The installed system (viz. CTCL/ IBT / DMA / SOR / STWT system) parameters are as per Exchange norms Gateway Parameters • • Trader ID • Market Segment - CM • • CTCL ID • • IP Address • • Exchange Network • • VSAT ID • Leased Line ID • Market Segment – F&O • • CTCL ID • • IP Address • • Exchange Network • • VSAT ID • • Leased Line ID • Market Segment – CDS • • CTCL ID • • IP Address • • Exchange Network • VSAT ID • Leased Line ID • Market Segment – CO • • CTCL ID • • IP Address • • Exchange Network • • VSAT ID • Leased Line ID	Yes	Yes
1	K	Trades Information The installed CTCL system provides a system based control facility over the trade confirmation process the 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	Yes	Yes
2		**Software Change Management - The system auditor should check whether proper procedures have been followed and proper documentation has been maintained for the following:**		
2	A	Processing / approval methodology of new feature request, change or patches	Yes	Yes

2	B	Change Management Process, related approvals, Version Control-History, etc. For change requests, whether the changes are tested before being approved for deployment into production. Whether the categorization of the change is done properly?	Yes	Yes
2	C	Fault reporting / tracking mechanism and process for resolution	Yes	Yes
2	D	1 Testing of new releases / patches / modified software / bug fixes	Yes	Yes
2	E	Does demonstratable segregation exists between Development / Test / Production environment 2 The System Auditor to check whether adequate mechanism to restore their trading systems to 'production state' at the end of testing session so as to ensure integrity of trading system.	Yes	Yes
2	F	New release in production – promotion, release note approvals	Yes	Yes
2	G	Production issues / disruptions reported during last year, reasons for such disruptions and corrective actions taken.	Yes	Yes
2	H	User Awareness	Yes	Yes
2	I	The system auditor should check whether critical changes made to the CTCL / IBT / STWT / ALGO / DMA /SOR etc.. are well documented and communicated to the Stock Exchange.	Yes	Yes

2	J	Change Management To ensure system integrity and stability all changes to the installed system are planned, evaluated for risk, tested, approved and documented. Has the organisation implemented a change management process to avoid risk due to unplanned and unauthorised changes for all the information security assets (Hardware, software, network, application)? Does the process at the minimum include the following? Planned Changes Are changes to the installed system made in a planned manner? a) Are they made by duly authorized personnel? b) Risk Evaluation Process c) 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? Emergency Changes In case of emergency changes, are the same duly authorized and the manner of change documented later? Are Records of all change requests maintained? Are periodic reviews conducted for all the changes which were implemented?	Yes	Yes

2	K	Patch Management Does the organization have a documented process/procedure for timely deployment of patches for mitigating identified vulnerabilities? Whether version and patch management controls are in place? 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?	Yes	Yes
2	L	SDLC - Application Development & Maintenance In case of members self-developed system SDLC documentation and procedures if the installed system is developed in-house	Yes	Yes
2	M	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?	Yes	Yes
2	N	Changes undertaken pursuant to a change to the stock Exchange's trading system.	Yes	Yes
2	O	The auditor should check that stock brokers are not using software without requisite approval of stock Exchange and there has not been any unauthorized change to the approved software.	Yes	Yes
3		**Risk Management System (RMS)**		
3	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 CTCL terminals (CTCL / IBT/ST WT / ALGO/SOR).	Yes	Yes
3	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.	Yes	Yes

3	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.	Yes	Yes
3	D	Order Review –Whether the system has capability to facilitate review of such orders that were not validated by the system.	Yes	Yes
3	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 pre-defined limits are captured by the system, documented and corrective steps taken.	Yes	Yes
3	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.	Yes	Yes
3	G	Order Reconfirmation Facility The installed CTCL 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	Yes	Yes
3	H	Settlement of Trades The installed CTCL system 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.	Yes	Yes

3	I	Information Risk Management Has the organization implemented a comprehensive integrated risk assessment, governance and management framework? Has the organization developed detailed risk management program that incorporates standards, guidelines, templates, processes, risk catalogues, checklist, measurement metrics and calendar to support and evidence risk management activities? If yes, is the risk management program calendar reviewed periodically? Are the risk identification and assessment processes repeated periodically to review existing risks and identify new risks Are risks reported to the Senior Management through reports and dashboards on a periodic basis? Are evidences available to demonstrate risk decisions such as Risk Mitigation, Risk Acceptance, Risk Transfer, Risk Avoidance by senior management. Is there a dedicated Risk Management Team for managing Risk and Compliance activities? Is the Risk Management Framework automated? Are SLA's defined for all risk management activities? Has the organization defined procedure/process for Risk Acceptance? Are reports and real time dashboards published in order to report/track Risks?	Yes	Yes
3	J	Has the organization deployed alert mechanism for detecting malfunctioning of device, software and backup system?	Yes	Yes
4		**Algorithmic Trading - The system auditor should check whether proper procedures have been followed and proper documentation has been maintained for the following:**		
4	A	Change Management –Whether any changes (modification/addition) to the approved Algos were informed to and approved by the exchange. The inclusion / removal of different versions of Algos should be well documented. Whether only approved strategy and software is used for the trading purpose	No	Yes
4	B	Online Risk Management capability- The ALGO server have capacity to monitor orders / trades routed through Algo trading and have online risk management for all	No	Yes

		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 may have following 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 / Maximum Order Size: • Daily 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 B) Client Level: • Cumulative Open Order Value check • Automated Execution check • Net position v/s available margins • 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 • Branch value limit for each branch ID • Security wise limit for each user ID • Identifying dysfunctional algorithms Does system has functionality to specify values as unlimited for any risk controls listed above? Does the member have additional risk controls / policies to ensure smooth functioning of the algorithm? (if yes, please provide details) • Immediate or cancel orders are not permitted for Commodity Derivative Segment • Market orders are not permitted at Commodity Derivative Segment • All orders generated by Algorithmic trading product adheres to the permissible limit of orders per second, if any as may be specified by SEBI /Exchange		

4	C	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. Integrity of all such logs is maintained, in other words logs should not be tampered	No	Yes
4	D	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.	No	Yes
4	E	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 or amounting to dysfunctional algo. The system should be capable to account for all execute, unexecuted and unconfirmed orders, placed by it before releasing further order(s). The system should have pre-defined parameters for an automatic stoppage in the event of algo leading to a loop or a runaway situation	No	Yes
4	F	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 stock broker is not using co-location/co-hosting facility in Commodity Derivatives Segment. The system auditor should verify that stock broker is not using Algorithmic trading from Exchange Hosted CTCL terminals in Commodity Derivatives Segment. Auditor should ensure that Commodity Derivatives trading is not done from Algo / Co-location facility	No	Yes

4	G	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 Stock Broker. 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.	No	Yes
4	H	Systems and Procedures – The system auditor should check and comment on the procedures, systems and technical capabilities of stock broker 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?	No	Yes
4	I	Reporting to Stock Exchanges – The system auditor should check whether the stock broker is informing the stock exchange regarding any incidents where the Algo has not behaved as expected. The system auditor should also comment upon the time taken by the stock broker to inform the stock exchanges regarding such incidents. (applicable for Commodity Derivatives segment). The system auditor should check whether stock broker make half yearly review of effect of approved strategies on liquidity and has surrender any such strategy which fails to induct liquidity (applicable for Commodity Derivatives segment)	No	Yes

4	J	Mock Testing or simulation testing: Have all approved Strategies for Algo trading, irrespective of the algorithm having undergone change or not, participated in the mock trading sessions or simulation minimum once a month?	No	Yes
4	K	Approved Strategy: Whether Members are placing Algo orders using only approved strategies. Whether all orders are with valid and approved strategy ID allocated by the Exchange	No	Yes
4	L	Liquidity Infusion Whether approved strategies not taking away liquidity from the market. Whether approved strategies are conducive to efficient price discovery or fair play in the market	No	Yes
4	M	Other Controls - Immediate or Cancel Orders are not permitted in Commodity Derivatives Segment using ATF - Market orders shall not be allowed to be placed in Commodity Derivatives Segment using ATF and only Limit Order should be placed using ATF. - 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. - 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 – 13th digit of CTCL field is populated as per published API?	No	Yes
4	N	The risk management system has the following model risk controls: 1. Circuit Breaker Check 2. Market Depth Check 3. Last Price Tolerance (LPT) Check 4. Fair Value Check	No	Yes

4	O	Whether member has submitted undertaking to the Exchange for performance/return claimed by unregulated platforms offering algorithmic strategies for trading as per SEBI circular no. SEBI/HO/MIRSD/DOP/P/CIR/2022/117 dated September 02, 2022 and member is not in violation in this regards	No	Yes
5		**Password Security**		
5	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 the API based terminals (CTCL terminals).	Yes	Yes
5	B	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.	Yes	Yes
5	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.	Yes	Yes

5	D	The installed CTCL Facility system Authentication mechanism is as per the guidelines of the Exchange The installed CTCL/IBT/DMA/SOR/STWT/ALGO system used password for authentication. The password policy/standard is documented. The installed systems password features includes: a) The installed system uses passwords for authentication. b) The system requests for identification and new password before login into the system. c) The Password is masked at the time of entry. System authenticates user with a User Name and password as first level of security. System mandates changing of password when the user logs in for the first time? Automatic disablement of the user on entering erroneous password on five consecutive occasions. The system provides for automatic expiry of passwords at the end of a reasonable duration (maximum 90 Days) and re-initialisation of access on entering fresh passwords. Prior intimation is given to the user before such expiry? 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 6 passwords. 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 minimum six characters. User/Client is deactivated if the same is not used for a continuous period of 12 (Twelve) months from date of last use of the account. System allows user to change their passwords at their discretion and frequency. System controls to ensure that the password is encrypted at member's end so that employees of the member cannot view the same at any point of time.	Yes	Yes
6		**Session Management (Mobile Application / Applicability Client Server Application / Web Application)**		
6	A	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.	Yes	Yes

6	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 WT only.	Yes	Yes
6	C	Inactive Session – Whether the system allows for automatic trading session logout after a system defined period of inactivity.	Yes	Yes
6	D	Log Management – Whether the system generates and maintain logs of Number of users, activity logs, system logs, Number of active clients.	Yes	Yes
6	E	The installed system has provision for security, reliability and confidentiality of data through use of encryption technology, SSL or similar session confidentiality protection mechanisms a) The system uses SSL/TLS or similar session confidentiality protection mechanisms b) The system uses a secure storage mechanism for storing of usernames and passwords c) The system adequately protects the confidentiality of the user's trade data.	Yes	Yes
6	F	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? Does the organization ensure that the data transferred through internet is protected with suitable encryption technologies? Are transactions on the website suitably encrypted?	Yes	Yes

6	G	Cryptographic Controls Is secret and confidential information sent through e-mails encrypted before sending? Is secret and confidential data in an encrypted format?	Yes	Yes
6	H	Does the organization have deployed data loss prevention (DLP)solutions / processes?	Yes	Yes
7		**Database Security**		
7	A	Access – Whether the system allows CTCL - database access only to authorized users / applications.	Yes	Yes
7	B	Controls – Whether the CTCL database server is hosted on a secure platform, with Username and password stored in an encrypted form using strong encryption algorithms.	Yes	Yes
7	C	Data at rest is encrypted	Yes	Yes
8		**Network Integrity**		
8	A	Seamless connectivity – Whether stock broker has ensured that a backup network link is available in case of primary link failure with the exchange.	Yes	Yes
8	B	Network Architecture – Whether the web server is separate from the Application and Database Server.	Yes	Yes
8	C	Firewall Configuration – Whether appropriate firewall is present between stock broker's trading setup and various communication links to the exchange. Whether the firewall default configuration settings are changed and is appropriately configured to ensure maximum security	Yes	Yes

8	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 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	Yes	Yes
9		**Access Controls**		
9	A	Access to server rooms – Whether adequate controls are in place for access to server rooms and proper audit trails are maintained for the same.	Yes	Yes
9	B	Additional Access controls – Whether the system provides for any authentication/two factor authentication mechanism to access to various components of the CTCL terminals (CTCL / IBT/ STWT / ALGO)respectively. Whether additional password requirements are set for critical features of the system. Whether the access control is adequate.	Yes	Yes

9	C	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? Whether adequate controls have been implemented for admission of personnel into the server rooms / place where servers / hardware / systems are located and whether audit trails of all the entries/exits at the server room / location are maintained? 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?	Yes	Yes
9	D	Extra Authentication Security If the systems uses additional authentication measures like smart cards, biometric authentication or tokens etc.	Yes	Yes

9	E	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 Center? 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 center?	Yes	Yes
9	F	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/deprovisioning reviewed?	Yes	Yes

9	G	Closed User Group Endpoint Security 1- Does the member have policies and procedures having coverage related to People, Processes and Technology? 2- Does the broker member have architecture that supports segregation such as Business - stock broking & Other business of stockbroker 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 Ensure appropriately configured firewalls are used to ensure segregation wherever needed. 3- Are technology related Baseline Controls established, exercised, and reviewed periodically 4- are following systems and processes existing and exercised for Vulnerability Assessment and Penetration Testing Configuration of Technologies prior to go live Monitoring of perimeter / network security, infrastructure and applications for anomalies alerts incidents and breaches Reporting of cyber-attacks, threats, cyber-incidents and breaches experienced and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities, threats to be submitted to stock exchange and other regulatory agencies based on applicability.	Yes	Yes
10		**Backup and Recovery**		
10	A	Backup and Recovery Policy – Whether the organization has a well documented policy on periodic backup of data generated from the broking operations.	Yes	Yes
10	B	Log generation and data consistency - Whether backup logs are maintained and backup data is tested for consistency.	Yes	Yes
10	C	System Redundancy – Whether there are appropriate backups in case of failures of any critical system components.	Yes	Yes

10	D	Backup & Restoration The Installed systems backup capability is adequate as per the requirements of the Exchange for overcoming loss of product integrity. Are backups of the following system generated files maintained as per the Exchange guidelines? At the server/gateway level a) Database b) Audit Trails Reports At the user level a) Market Watch b) Logs c) History d) Reports e) Audit Trails f)Alert logs 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 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 for SOR capture the record of orders, trades and data points for the basis of routing decision? Are backup procedures documented and backup logs maintained? Are the backup logs maintained and are the backups been verified and tested? 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?	Yes	Yes
10	E	Audit trail, Event logging and monitoring o Member should maintain logs of all trading activity to facilitate audit trail. o Whether system generates, captures and maintains audit trail of all transactions for at least 3 years? o Audit trail should capture record of control parameters, orders, trades and data points emanating from trades executed through algorithmic trading? o All events, changes in master, strategy parameters shall be logged and maintained for at least 3 years. o Whether all logs generated are secured from unauthorized modifications?	Yes	Yes

10	F	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 Exchange? 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 an alternate communications path between the firm and its employees? Is there an alternate communications path with critical business constituents, banks and regulators? Whether detailed network diagram is prepared and available for verification? Is network and network diagram in line with the one submitted to the Exchange? 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.	Yes	Yes

10	G	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 a) Gateway / Database Server b) Router c) Network Switch Infrastructure breakdown backup Are there suitable arrangements made for the breakdown in any infrastructure components like d) Power Supply e) Water f) 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?	Yes	Yes
11		**BCP/DR (Only applicable for Stock Brokers having BCP / DR site)**		
11	A	BCP / DR Policy – Whether the stock broker has a well-documented BCP/ DR policy and plan. The system auditor should comment on the documented incident response Exchange procedures.	Yes	Yes
11	B	Alternate channel of communication – Whether the stock broker 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).	Yes	Yes

11	C	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.	Yes	Yes
11	D	Connectivity with other FMIs – The system auditor should check whether there is an alternative medium to communicate with Stock Exchanges and other FMIs.	Yes	Yes
11	E	Business Continuity Does the Organisation have a suitable documented Business Continuity or Disaster Recovery or Incident Response process commensurate with the organization size and risk profile to ensure a high degree of availability of the installed system Is there any documentation on Business Continuity / Disaster Recovery / Incident Response? If a BCP/DRP plan exists, has it been tested on regular basis? Are there any documented risk assessments? Does the installation have a Call List for emergencies maintained? Whether redundancy is built at all level of infrastructure? Whether all critical systems / infrastructure are in HA mode?	Yes	Yes
11	F	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?	Yes	Yes
11	G	Security Incident & Event Management Is there a dedicated Incident Response Team for managing risk and compliance activities?	Yes	Yes
11	H	Business Continuity Does the organization have a Disaster Recovery Site? Are there any documented risk assessments? Does the installation 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?	Yes	Yes

11	I	1. 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.	Yes	Yes
11	J	1. 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? 2.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?	Yes	Yes
12		**Segregation of Data and Processing facilities**		
12	A	The system auditor should check and comment on the segregation of data and processing facilities at the Stock Broker in case the stock broker is also running other business.	Yes	Yes
13		**Back office data**		
13	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.	Yes	Yes
13	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.	Yes	Yes

14		**User Management**		
14	A	User Management Policy – The system auditor should check whether the stock broker has a well-documented policy that provides for user management and the user management policy explicitly defines user, database and application Access Matrix.	Yes	Yes
14	B	Access to Authorized users – The system auditor should check whether the system allows access only to the authorized users of the CTCL 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.	Yes	Yes
14	C	User Creation / Deletion – The system auditor should check whether new user ids were created / deleted as per CTCL guidelines of the exchange and whether the user ids are unique in nature.	Yes	Yes
14	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.	Yes	Yes
14	E	User Management system: User Deletion: Users are deleted as per the Exchange guidelines 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	Yes	Yes
15		**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))**		
15	A	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.	Yes	Yes
15	B	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.	Yes	Yes

15	C	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	Yes	Yes
15	D	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.	Yes	Yes
15	E	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?	Yes	Yes
15	F	To ensure information security for the Organization in general and the installed system in particular policy and procedures as per the Exchange 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 Exchange 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 Management Policy Audit Trail Policy Capacity Management Plan Does the organization follow any other policy or procedures or documented practices that are relevant?	Yes	Yes

15	G	Are documented practices available for various system processes Day Begins Day Ends Other system processes a) Audit Trails b) Access Logs c) Transaction Logs d) Backup Logs e) Alert Logs f) Activity Logs g) Retention Period h) Data Maintenance	Yes	Yes
15	H	In case of failure, is there an escalation procedure implemented? Day Begin Day End Other system processes Details of the various response procedures including for a) Access Control failure b) Day Begin failure c) Day End failure d) Other system Processes failure	Yes	Yes
15	I	Vulnerability Assessment, Penetration Testing & Application Security Assessments: Are periodic vulnerability assessments for all the critical assets including Servers, OS, Database, Middleware, Network Devices, Firewalls, IDS /IPS etc conducted?	Yes	Yes
15	J	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?	Yes	Yes

15	K	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?	Yes	Yes
15	L	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?	Yes	Yes
15	M	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?	Yes	Yes
15	N	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?	Yes	Yes
15	O	Does the organisation have hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments.	Yes	Yes
15	P	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?	Yes	Yes
15	Q	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.?	Yes	Yes
15	R	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?	Yes	Yes

15	S	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?	Yes	Yes
16		**Software Testing Procedures - The system auditor should check whether the stock broker has complied with the guidelines and instructions of SEBI / stock exchanges with regard to testing of software and new patches, including the following:**		
16	A	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.	Yes	Yes
16	B	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.	Yes	Yes
16	C	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.	Yes	Yes
17		**Additional Points**		
17	A	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?	Yes	Yes

17	B	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	Yes	Yes
17	C	The installed system 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 systems has a provision for On-line surveillance and risk management as per the requirements of Exchange and includes Number of Users Logged In / hooked on to the network incl. privileges of each The installed systems has a provision for off line monitoring and risk management as per the requirements of Exchange and includes reports / logs on a) Number of Authorized Users b) Activity logs c) Systems logs d) Number of active clients	Yes	Yes
17	D	Insurance The insurance policy of the Member covers the additional risk of usage of system and probable losses in case of software malfunction	Yes	Yes
17	E	Firewall Whether suitable firewalls are implemented? Are the rules defined in the firewall adequate to prevent unauthorized access to IBT/DMA/STWT systems	Yes	Yes

17	F	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 CTCL/ALGO/IBT/DMA/STWT/SOR orders are located in India. Provide address of the CTCL / IBT / DMA / SOR / STWT server location (as applicable) Whether the required details of all the CTCL facility 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 CTCL facility user ids created in the server of the trading member have been mapped to 12 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 CTCL terminals (CTCL/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 – 13th digit of field is populated appropriately. Whether every algorithm order reaching on exchange platform is tagged with the unique identifier allotted to the respective algorithm by the Exchange. All orders routed through CTCL/IBT/STWT/DMA/SOR/ALGO 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 : · The limits are setup after assessing the risks of the	Yes	Yes

		corresponding user ID and branch ID · The limits are setup after taking into account the member's capital adequacy requirements · All the limits are reviewed regularly and the limits in the system are up to date · All the branch or user have got limits defined and that No user or branch in the system is having unlimited limits on the above stated parameters · Daily record of these limits is preserved and shall be produced before the Exchange as and when the information is called for · Compliance officer of the member has certified the above in the quarterly compliance certificate submitted to the Exchange IBT/STWT Compliance: Does the broker's IBT / STWT system complies with the following provisions : · The system captures the IP (Internet Protocol) address (from where the orders are originating), for all IBT/ STWT orders · The system has built-in high system availability to address any single point failure · The system has secure end-to-end encryption for all data transmission between the client and the broker system through a Secure Standardized Protocol. A procedure of mutual authentication between the client and the broker server is implemented · The system has adequate safety features to ensure it is not susceptible to internal/ external attacks · In case of failure of IBT/ STWT, the alternate channel of communication has adequate capabilities for client identification and authentication · Two-factor authentication for login session has been implemented for all orders emanating using Internet Protocol · In case of no activity by the client, the system provides for automatic trading session logout · The back-up and restore systems implemented by the broker is adequate to deliver sustained performance and high availability. The broker system has on-site as well as remote site back-up capabilities · Name of the website provided in the application form is the website through which Internet based trading services is to be provided to the clients. · Secured socket level security for server access through Internet is available. · SSL certificate is valid and trading member is the owner of the website provided.		

		Any change in name of the website or ownership of the website shall be incorporated only on approval from the Exchange - Whether the order routing servers routing CTCL/ALGO/IBT/WT/DMA/SOR orders are located in India and through specified CTCL / ATS User ID approved by the Exchange for Trading - ATF software / IDs do not have any interlink with any system or ID located / linked outside India. - Whether the required details of all the CTCL 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 CTCL user ids created in the server of the trading member have been mapped to 12 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 CTCL terminals (CTCL/IBT/WT/ALGO) are offered to the market for matching and system does not have any order matching function resulting into cross trades. - All orders routed through CTCL / IBT / WT 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.		
17	G	Vendor Certified Network diagram Date of submission of network diagram to Exchange (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	Yes	Yes

17	H	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?	Yes	Yes
17	I	DOS Does the organization periodically conduct mock DOS scenarios to have insight into the preparedness in tackling with DOS/DDOS attacks?	Yes	Yes
17	J	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?	Yes	Yes
17	K	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	Yes	Yes
17	L	Independent Audits Are periodic independent audits conducted by Third Party / internal Auditors? Are the audit findings tracked to closure?	Yes	Yes

17	M	Human Resources Security, Acceptable Usage & Awareness Trainings Are periodic surprise audits and social engineering attacks conducted to assess security awareness of employees and vendors? 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 reviewed and 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?	Yes	Yes
18		**AI-ML**		
18	A	Are adequate safeguards in place to prevent abnormal behavior of the AI or ML application / System.	Yes	Yes
18	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.	Yes	Yes
18	C	Whether AI / ML systems comply for all above System Audit Checklist points. In case of any observation, please report.	Yes	Yes
19		**The system has been installed after complying with the various Exchanges circulars issued from time to time** Copy of Undertaking provided regarding the CTCL 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 (SOR)	Yes	Yes
20		**Pre Trade Risk Control** Whether appropriate pre-trade checks, alerts, and controls are built in CTCL facility/ systems such that an alert shall be generated if the user places limit order at a price which is away from prevailing market prices.	Yes	Yes

21		**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?	Yes	Yes
22		**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?	Yes	Yes
23		**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 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	Yes	Yes

24		**MongoDB and Elasticsearch server Controls:**		
24	A	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.	Yes	Yes
24	B	ii. Use TLS/SSL for all incoming and outgoing connections including communication between internal components of MongoDB as well as between applications and MongoDB.	Yes	Yes
24	C	iii. Encrypt the MongoDB data stored in the storage layer and use appropriate file system permissions to restrict access to the data.	Yes	Yes
24	D	iv. 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.	Yes	Yes
24	E	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.	Yes	Yes
25		**Internal Policy Controls for Technical Glitch**		
25	A	Does the organisation have internal policy to handle technical glitches?	Yes	Yes
25	B	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.	Yes	Yes
26		**Remote Access Controls**		
26	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?	Yes	Yes

26	B	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?	Yes	Yes
26	C	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?	Yes	Yes
26	D	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?	Yes	Yes
26	E	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.	Yes	Yes
26	F	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?	Yes	Yes
26	G	Does the organization have appropriate risk mitigation mechanisms whenever remote access of data center resources is permitted for service providers?	Yes	Yes
26	H	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?	Yes	Yes
26	I	Does the organizations backup, restore and archival functions work seamlessly, particularly if the users have remote access to internal systems.?	Yes	Yes
26	J	Does the organization apply only necessary and applicable patches to the existing hardware and software?	Yes	Yes

26	K	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?	Yes	Yes
26	L	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, Exchange, 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	Yes	Yes
27		**SEBI and Exchange Compliances**		
27	A	Auditor to list all applicable Circulars, Notices, Guidelines, and advisories published by SEBI and Exchanges and mention	Yes	Yes
27	B	1- Adherence to all such Circulars, Notices, Guidelines, and advisories published	Yes	Yes
27	C	2- Reporting adherences based on prescribed periodicity in point 1 above	Yes	Yes

Annexure B

Terms of Reference for Cyber Security & Cyber Resilience Audit

Section	Sub Section	Area of Verification
1		**Governance**
1	A (i)	Whether the Stockbroker has formulated a comprehensive Cyber Security and Cyber Resilience policy document encompassing the framework mentioned in the circular?
	A (ii)	In case of deviations from the suggested framework, whether reasons for such deviations, technical or otherwise, are provided in the policy document?
	A (iii)	Is the policy document approved by the Board / Partners / Proprietor of the organization?
	A (iv)	Whether the policy document is reviewed by the aforementioned group at least annually with the view to strengthen and improve its Cyber Security and Cyber Resilience framework.
	A (v)	Policy Approval Date
	A (vi)	Policy Version
	A (vii)	Policy Approval By
1	B (i)	Whether the Cyber Security Policy includes the following process to identify, assess, and manage Cyber Security risk associated with processes, information, networks, and systems:
	B (ii)	a. 'Identify' critical IT assets and risks associated with such assets.
	B (iii)	b. 'Protect' assets by deploying suitable controls, tools, and measures.
	B (iv)	c. 'Detect' incidents, anomalies, and attacks through appropriate monitoring tools/processes.
	B (v)	d. 'Respond' by taking immediate steps after identification of the incident, anomaly, or attack.
	B (vi)	e. 'Recover' from incident through incident management and other appropriate recovery mechanisms.
1	C	Whether policy / Procedure document refers to best practices from international standards like ISO 27001, COBIT 5, etc., or their subsequent revisions, if any, from time to time.
1	D	Whether policy document have considered the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organization (NTRO), Government of India (titled 'Guidelines for Protection of National Critical Information Infrastructure') and subsequent revisions, if any, from time to time.

1	E	Stockbrokers / Depository Participants should designate a senior official or management personnel (henceforth, referred to as the "Designated Officer") whose function would be to assess, identify, and reduce security and Cyber Security risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the Cyber Security Policy.
1	F (i)	Whether the Member has constituted an Technology Committee comprising experts.
	F (ii)	This Technology Committee has reviewed on a half yearly basis the implementation of the Cyber Security and Cyber Resilience policy, which includes:
	F (iii)	- review of their current IT and Cyber Security and Cyber Resilience capabilities,
	F (iv)	- if committee has set goals for a target level of Cyber Resilience and establish plans to improve and strengthen Cyber Security and Cyber Resilience.
	F (v)	- And the review report is placed before the Board / Partners / Proprietor of the Stockbrokers / Depository Participants for appropriate action.
1	G	Whether the Designated officer and the technology committee periodically reviewed instances of cyber-attacks, if any, domestically and globally, and taken steps to strengthen Cyber Security and cyber resilience framework.
1	H	Whether Brokers / Depository Participants has policy or reporting procedure to facilitate communication of unusual activities and events to the Designated Officer in a timely manner.
1	I	Has Stockbroker/Depository Participant defined and documented roles and responsibilities of its employees, outsourced staff, and employees of vendors, members or participants and other entities, who may have privileged access or use systems / networks of the Stockbroker/Depository Participants towards ensuring the goal of Cyber Security?
1	J	Stockbrokers / Depository Participants should prepare detailed incident response plan and define roles and responsibilities of Chief Information Security Officer (CISO) and other senior personnel. Reporting and compliance requirements shall be clearly specified in the security policy. In addition, share the details of CISO with CERT-In through Email (info AT cert-in.org.in)

2		**Identification**
2	A	Has the Stock Broker / Depository Participant identified and classified critical assets based on their sensitivity and criticality for business operations, services and data management. The critical assets shall include business critical systems, internet facing applications /systems, systems that contain sensitive data, sensitive personal data, sensitive financial data, Personally Identifiable Information (PII) data, etc. All the ancillary systems used for accessing/communicating with critical systems either for operations or maintenance shall also be classified as critical system. The Board/Partners/Proprietor of the Stock Brokers / Depository Participants shall approve the list of critical systems. To this end, Stock Brokers / Depository Participants should maintain up-to-date inventory of its hardware and systems and the personnel to whom these have been issued, software and information assets (internal and external), details of its network resources, connections to its network and data flows.
2	B	Has the Stockbrokers / Depository Participants identified / has process to identify cyber risks (threats and vulnerabilities) that it may face, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.
3		**Protection**
3	A	Access control No person by virtue of rank or position should have any intrinsic right to access Confidential data, applications, system resources or facilities.
3	B	Any and all access to Stockbrokers / Depository Participants systems, applications, networks, databases etc., have defined purpose and for a defined period. Stockbrokers / Depository Participants should grant access to IT systems, applications, databases, and networks on a need-to-use basis and based on the principle of least privilege to provide security for both on-and off-premises resources (i.e. zero-trust models). Such access should be for the period when the access is required and should be authorized using strong authentication mechanisms.
3	C	Have Stockbrokers / Depository Participants implemented an access policy which addresses strong password controls for users' access to systems, applications, networks, and databases. Illustrative examples for this are given in Annexure C of SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018
3	D	All critical systems of the Stockbroker / Depository Participant accessible over the internet should have two-factor security (such as VPNs, Firewall controls etc.)

3	E	Stockbrokers / Depository Participants should ensure that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes. Such logs should be maintained and stored in a secure location for a time period not less than two (2) years.
3	F	Stockbrokers / Depository Participants should deploy controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users) to Stockbroker / Depository Participant's critical systems. Such controls and measures should inter-alia include restricting the number of privileged users, periodic review of privileged users' activities, disallow privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.
3	G	Employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to the Stockbrokers / Depository Participants critical systems, networks, and other computer resources, should be subject to stringent supervision, monitoring, and access restrictions.
3	H	Stockbrokers / Depository Participants should formulate an Internet access policy to monitor and regulate the use of internet and internet-based services such as social media sites, cloud-based internet storage sites, etc. within the Stockbroker / Depository Participant's critical IT infrastructure.
3	I	User Management must address deactivation of access of privileges of users who are leaving the organization or whose access privileges have been withdrawn.
4		**Physical Security**
4	A	Physical access to the critical systems should be restricted to minimum and only to authorized officials. Physical access of outsourced staff/visitors should be properly supervised by ensuring at the minimum that outsourced staff/visitors are always accompanied by authorized employees.
4	B	Physical access to the critical systems should be revoked immediately if the same is no longer required.
4	C	Stockbrokers/ Depository Participants has ensured that the perimeter of the critical equipment's room, if any, are physically secured and monitored by employing physical, human, and procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. where appropriate

5		Network Security Management
5	A	Stockbrokers / Depository Participants has established baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within their IT environment.
5	B	The LAN and wireless networks should be secured within the Stockbrokers /Depository Participants' premises with proper access controls.
5	C	For algorithmic trading facilities, adequate measures should be taken to isolate and secure the perimeter and connectivity to the servers running algorithmic trading applications.
5	D	Stockbrokers / Depository Participants should install network security devices, such as firewalls, proxy servers, intrusion detection and prevention systems (IDS) to protect their IT infrastructure which is exposed to the internet, from security exposures originating from internal and external sources.
5	E	Adequate controls must be deployed to address virus / malware / ransomware attacks. These controls may include host / network / application-based IDS systems, customized kernels for Linux, anti-virus, and anti-malware software etc.
6		**Data security**
6	A	Critical data must be identified and encrypted in motion and at rest by using strong encryption methods. Illustrative measures in this regard are given in Annexure A and B of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018
6	B	Stockbrokers / Depository Participants should implement measures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity. It should be ensured that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties. Illustrative measures to ensure security during transportation of data over the internet are given in Annexure B of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018

6	C	The information security policy should also cover use of devices such as mobile phones, faxes, photocopiers, scanners, etc., within their critical IT infrastructure, that can be used for capturing and transmission of sensitive data. For instance, defining access policies for personnel, and network connectivity for such devices etc.
6	D	Stockbrokers / Depository Participants should allow only authorized data storage devices within their IT infrastructure through appropriate validation processes.
6	E	Stockbrokers / Depository Participants should Enforce BYOD (Bring your own device) security policies, like requiring all devices to use a business-grade VPN service and antivirus protection
6	F	Stockbrokers/ Depository Participants shall deploy detection and alerting tools. Members shall create process to prevent, contain and respond to a data breach/ data leak.
7		**Hardening of Hardware and Software**
7	A	Whether Member only deploys hardened hardware / software, including replacing default passwords with strong passwords and disabling or removing services identified as unnecessary for the functioning of the system.
7	B	Whether Open ports on networks and systems which are not in use or that can be potentially used for exploitation of data should be blocked and measures taken to secure them.
8		**Application Security in Customer Facing Applications**
8	A	Whether over the Internet application like IBTs (Internet Based Trading applications) portal and back-office application, containing sensitive or private information are secured by using security measures. (Illustrative list of measures for ensuring security in such applications is provided in Annexure C of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018

9		**Certification of off-the-shelf products**
9	A	Stockbrokers / Depository Participants should ensure that off the shelf products being used for core business functionality (such as Back-office applications) should 1. bear Indian Common criteria certification of Evaluation Assurance Level 4. The Common criteria certification in India is being provided by (STQC) Standardisation Testing and Quality Certification (Ministry of Electronics and Information Technology). or 2. Certified independently on criteria similar to Indian Common Criteria Certificate of Evaluation Assurance Level. Custom developed / in-house software and components need not obtain the certification, but must undergo intensive regression testing, configuration testing etc. The scope of tests should include business logic and security controls.
10		**Patch management**
10	A	Stockbrokers / Depository Participants should establish and ensure that the patch management procedures include the identification, categorization and prioritization of patches and updates. An implementation timeframe for each category of patches should be established to apply them in a timely manner.
10	B	Stockbrokers / Depository Participants should perform rigorous testing of security patches and updates, where possible, before deployment into the production environment to ensure that the application of patches do not impact other systems.
11		**Disposal of data, systems, and storage devices**
11	A	Stockbrokers / Depository Participants should frame suitable policy for disposal of storage media and systems. The critical data / Information on such devices and systems should be removed by using methods such as crypto shredding / degauss / Physical destruction as applicable.
11	B	Stockbrokers / Depository Participants should formulate a data-disposal and data-retention policy to identify the value and lifetime of various parcels of data.
12		**Vulnerability Assessment and Penetration Testing (VAPT)**
12	A	Stock Brokers / Depository Participants shall carry out periodic Vulnerability Assessment and Penetration Tests (VAPT) which inter-alia include critical assets and infrastructure components like Servers, Networking systems, Security devices, load balancers, other IT systems pertaining to the activities done as Stock Brokers / Depository Participants etc., in order to detect security vulnerabilities in the IT environment and in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks

12	B	Stock Brokers / Depository Participants shall conduct VAPT at least once in a financial year. All Stock Brokers / Depository Participants are required to engage only CERT-In empaneled organizations for conducting VAPT. The final report on said VAPT shall be submitted to the Stock Exchanges / Depositories after approval from Technology Committee of respective Stock Brokers / Depository Participants, within 1 month of completion of VAPT activity.
12	C	In addition, Stock Brokers / Depository Participants shall perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system which is a critical system or part of an existing critical system.
12	D	In case of vulnerabilities discovered in off-the-shelf products (used for core business) or applications provided by exchange empaneled vendors, Stockbrokers / Depository Participants should report them to the vendors and the exchanges in a timely manner.
12	E	Any gaps/vulnerabilities detected shall be remedied on immediate basis and compliance of closure of findings identified during VAPT shall be submitted to the Stock Exchanges / Depositories within 3 months post the submission of final VAPT report
13		**Monitoring and Detection**
13	A	Stockbrokers / Depository Participants should establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events / alerts and timely detection of unauthorised or malicious activities, unauthorised changes, unauthorised access and unauthorised copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices exposed to the internet should also be monitored for anomalies.
13	B	Further, to ensure high resilience, high availability, and timely detection of attacks on systems and networks exposed to the internet, Stockbrokers / Depository Participants should implement suitable mechanisms to monitor capacity utilization of its critical systems and networks that are exposed to the internet, for example, controls such as firewalls to monitor bandwidth usage.
14		**Response and Recovery**
14	A	Alerts generated from monitoring and detection systems should be suitably investigated to determine activities that are to be performed to prevent expansion of such incident of cyber-attack or breach, mitigate its effect, and eradicate the incident.
14	B	The response and recovery plan of the Stockbrokers / Depository Participants should have plans for the timely restoration of systems affected by incidents of cyber-attacks or breaches, for instance, offering alternate services or systems to Customers. Stockbrokers / Depository Participants should have the same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as specified by SEBI for Market Infrastructure Institutions vide SEBI circular CIR/MRD/DMS/17/20 dated June 22, 2012 as amended from time to time
14	C	The response plan should define responsibilities and actions to be performed by its employees and support / outsourced staff in the event of cyber-attacks or breach of Cyber Security mechanism.

14	D	Any incident of loss or destruction of data or systems should be thoroughly analyzed
14	E	And lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes.
14	F	Stockbrokers / Depository Participants should also conduct suitable periodic drills to test the adequacy and effectiveness of the response and recovery plan.
15		**Sharing of Information**
15	A	All Cyber-attacks, threats, cyber-incidents and breaches experienced by Stock Brokers / Depositories Participants shall be reported to Stock Exchanges / Depositories /CERT-IN & SEBI within 6 hours of noticing / detecting such incidents or being brought to notice about such incidents. This information shall be shared to SEBI through the dedicated e-mail id: incident@cert-in.org.in & sbdp-cyberincidents@sebi.gov.in.
15	B	The incident shall also be reported to Indian Computer Emergency Response team (CERT-In) in accordance with the guidelines / directions issued by CERT-In from time to time. Additionally, the Stock Brokers / Depository Participants, whose systems have been identified as "Protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC.
15	C	The quarterly reports containing information on cyber-attacks, threats, cyber-incidents and breaches experienced by Stock Brokers / Depository Participants and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities, threats that may be useful for other Stock Brokers / Depository Participants / Exchanges /Depositories and SEBI, shall be submitted to Stock Exchanges / Depositories within 15 days from the quarter ended June, September, December and March of every year.
16		**Training and Education**
16	A	Stockbrokers / Depository Participants should work on building Cyber Security and basic system hygiene awareness of staff (with a focus on staff from non-technical disciplines).
16	B	Stockbrokers / Depository Participants should conduct periodic training programs to enhance knowledge of IT / Cyber Security Policy and standards among the employees incorporating up-to-date Cyber Security threat alerts. Where possible, this should be extended to outsourced staff, vendors etc.
16	C	The training programs should be reviewed and updated to ensure that the contents of the program remain current and relevant.
16	D	Stockbrokers / Depository Participants should Provide training to the employees to avoid clicking on a link in a spear-phishing email, reusing their personal password on a work account, mixing personal with work email and/or work documents, or allowing someone they shouldn't to use their corporate device- especially in Work from Home environments.

17		**Systems managed by vendors**
17	A	Where the systems (IBT, Back office and other Customer facing applications, IT infrastructure, etc.) of a Stock Brokers / Depository Participants are managed by vendors and the Stock Brokers / Depository Participants may not be able to implement some of the aforementioned guidelines directly, the Stock Brokers / Depository Participants should instruct the vendors to adhere to the applicable guidelines in the Cyber Security and Cyber Resilience policy and obtain the necessary self-certifications from them to ensure compliance with the policy guidelines.
18		**SEBI and Exchange Compliances**
18	A	Auditor to list all applicable Circulars, Notices, Guidelines, and advisories published by SEBI and Exchanges and mention
18	B	1- Adherence to all such Circulars, Notices, Guidelines, and advisories published
18	C	2- Reporting adherences based on prescribed periodicity in point 1 above
19		**Advisory for Financial Sector Organizations:**
19	A	Whether compliance of the SEBI circular no. SEBI/HO/MIRSD2/DOR/CIR/P/ 2020/221 dated November 03, 2020 for Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions has been made.
20		**Cyber Security Advisory - Standard Operating Procedure (SOP)**
20	A	Cyber Security Advisory – Standard Operating Procedure (SOP) for handling cyber security incidents of intermediaries-as per SEBI directives. The aspects which shall form part of the SOP and whether stock-broker has to complied.
20	B	Members shall have a well-documented Cyber Security incident handling process document (Standard Operating Procedure - SOP) in place. Such policy shall be approved by Board of the Member (in case of corporate trading member), Partners (in case of partnership firms) or Proprietor (in case of sole proprietorship firm) as the case may be and shall be reviewed annually by the "Internal Technology Committee" as constituted under SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 for review of Security and Cyber Resilience policy.
20	C	Members shall examine the Cyber Security incident and classify the Cyber Security incidents into High/ Medium/ Low as per their Cyber Security incident handling process document. The Cyber Security incident handling process document shall define decision on Action/ Response for the Cyber Security incident based on severity.
20	D	Members shall report the Cyber Security incident to Indian Computer Emergency Response Team (CERT-In).

20	E	Members shall provide the reference details of the reported Cyber Security incident with CERTI n to the Exchange and SEBI. Members shall also provide details, regarding whether CERT-In team is in touch with the Member for any assistance on the reported Cyber Security incident. If the Cyber Security incident is not reported to CERT-In, members shall submit the reasons for the same to the Exchange and SEBI. Members shall communicate with CERT-In/ Ministry of Home Affairs (MHA)/ Cyber Security Cell of Police for further assistance on the reported Cyber Security incident.
20	F	Members shall submit details whether Cyber Security incident has been registered as a complaint with law enforcement agencies such as Police or its Cyber Security cell. If yes, details need to be provided to Exchange and SEBI. If no, then the reason for not registering complaint shall also be provided to Exchange and SEBI.
20	G	The details of the reported Cyber Security incident and submission to various agencies by the Members shall also be submitted to Division Chiefs (in-charge of divisions at the time of submission) of DOS-MIRSD and CISO of SEBI
20	H	The Designated Officer of the Member (appointed in terms of para 6 of the aforementioned SEBI Circular dated December 03, 2018) shall continue to report any unusual activities and events within 6 hours of receipt of such Information as well as submit the quarterly report on the cyber-attacks & threats within 15 days after the end of the respective quarter in the manner as specified in Exchange circular.
21		**TECHNICAL GLITCH**
21	A	Member has reported all instances of technical glitches within the prescribed timelines during the audit period in accordance with regulatory guidelines. Member has correctly reported the issues faced and duration of the downtime. Member has implemented all the measures as mentioned in RCAs and has taken necessary steps to prevent the recurrence of such technical glitch.