NATIONAL STOCK EXCHANGE OF INDIA LIMITED

DEPARTMENT : CAPITAL MARKET SEGMENT	
Download Ref No : NSE/CMTR/26285	Date : March 25, 2014
Circular Ref. No : 18/2014	

All Members,

Sub: System Audit of Stock Brokers / Trading Members

SEBI has specified systems audit requirement for stock brokers / trading members vide circular CIR/MRD/DMS/34/2013 dated November 06, 2013. As per the provisions of the circular stock brokers/ trading members using trading software shall be required to do the following:

i. Carry out System audit of their trading facility as per applicability criteria (Annexure - A)
ii. Such system audit of trading system shall be undertaken by a system auditor who fulfills the eligibility norms. (Annexure - B)
iii. Obtain Preliminary system audit report from the system auditor as per the format given in Executive Summary Reporting (Annexure - C) through ENIT.
iv. Forward Annexure - C to the Exchange after adding Management comments in the space provide through ENIT.
v. Take corrective action for the observations made by the system auditor on non-compliance / non-conformities (NCs), if any, in the Preliminary report and submit Action Taken Report (ATR) in the space provided through ENIT.
vi. If the Follow-on audit has been recommended by the auditor in Preliminary audit report, then schedule the same after taking necessary corrective actions and submit the Follow-on Audit Report as per Annexure - D to the Exchange through ENIT.
vii. The time lines (on or before) for submission of Preliminary audit report, Action Taken Report (ATR) and Follow-on audit report is as given in the following table:

Audit Period	**Preliminary Audit Report (Annexure - C)**	**Action taken Report (ATR) (if applicable)**	**Follow-on Audit Report (if applicable) (Annexure - D)**
Half Yearly (April-September)	October 31	November 30	December 31
Half Yearly (October-March)	April 30	May 31	June 30
Annual (April-March)	April 30	May 31	June 30
Once in 2 years (April-March for 24 Months)	April 30	May 31	June 30

For any clarifications please call Toll free number 1800 2200 53.

For and on behalf of
National Stock Exchange of India Ltd.

Suprabhat Lala
Vice President

Toll free number	**Fax No**	**Email id**
1800 2200 53	022-2659 8447	backoffice@nse.co.in

Annexure - A

S No.	Category of Member	Members using the trading software							
		Only NEAT		Both NEAT and NNF and presence in < 10 locations and have < 50 terminals		Both NEAT and NNF and presence in > 10 locations or have > 50 terminals		NEAT, NNF and ALGO (irrespective of location and terminals)	
		Terms of Reference (ToR)	Frequency of audit	Terms of Reference (ToR)	Frequency of audit	Terms of Reference (ToR)	Frequency of audit	Terms of Reference (ToR)	Frequency of audit
1	Stock Brokers / Trading Members	Type - I	Once in 2 years	Type - II	Once in 2 years	Type - II	Annual	Type - III	Half yearly
2	Stock Broker/Trading Members who are also depository participants or are involved in offering any other financial services	Type - I	Annual	Type - II	Annual	Type - II	Annual	Type - III	Half yearly

For members falling under the category "Only NEAT" i.e. using only NEAT trading software, the first such audit period shall be from April 01, 2013 to 31st March 2015.

Terms of Reference (ToR) is given in Annexure - E

Annexure - B

Auditor Selection Norms

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

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

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

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

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

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

Annexure - C

Executive Summary Reporting

(To be on the letterhead of the system auditor)

System Audit Report for the period _____ to _____)

I/We, M/s. _____ (Name of the system auditor / system audit firm) have conducted the system audit of Trading system facility/ies of the below mentioned trading member of National Stock Exchange in accordance with the provisions and scope laid down by the Exchange in Annexure-A. The detailed audit report has been submitted to the trading member. The summary of findings are grouped under the broad categories as below and classified as 'High Risk', 'Medium Risk' or 'Low Risk'.

NSE Trading Member Code: _____

NSE Trading Member Name: _____

Audit Date	Observation No	Description of Finding / Observations	Dept.	Status / Nature of Findings	Risk Rating of Findings	Audit TOR Clause	Audited By	Root Cause Analysis	Impact Analysis	Suggested Corrective Action	Deadline for the Corrective Action	Follow-on Audit required (Yes / No)	Verified By	Closing Date	Trading Member Management Comments

Declaration:

- All the branches/locations trading software facility is provided have been audited and ONE consolidated report has been submitted for all market segments.
- There is no conflict of interest with respect to the member being audited. If any such instance arises, it shall be brought to the notice of the Exchange immediately before undertaking the audit.
- With regard to the areas mentioned in the Terms of Reference (ToR), compliance / non-compliance status has been specified. Observations on minor / major deviations as well as qualitative comments for scope for improvement also have been specified in the report.

Signature

Countersigned by Member

(Name of the Auditor & Auditing firm)
CISA / DISA / CISM / CISSP Reg. No. :

Authorized signatory

Date:

Place:

Stamp / Seal

Description of relevant Table heads:

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

2. **Description of Findings/ Observations** – Description of the findings in sufficient detail, referencing any accompanying evidence (e.g. copies of procedures, interview notes, screen shots etc.)

3. **Status and Nature of findings –** The category can be specified as (a) Non-Compliant (b) Work In Progress (c) Observation (d) Suggestions

4. **Risk Rating of Findings –** A rating has to been given for each of the observations based on their impact and severity to reflect the risk exposure, as well as the suggested priority for action.

Rating	**Description**
HIGH RISK	Weakness in control those represent exposure to the organization or risks that could lead to instances of non-compliance with the requirements of TORs. These risks need to be addressed with utmost priority.
MEDIUM RISK	Potential weakness in controls, which could develop into an exposure or issues that represent areas of concern and may impact internal controls. These should be addressed reasonably promptly.
LOW RISK	Potential weaknesses in controls, which in combination with other weakness can develop into an exposure. Suggested improvements for situations not immediately/directly affecting controls.

5. **Audit TOR Clause –** The TOR clause corresponding to this observation

Annexure- D

Follow on System Audit Report

(To be on the letterhead of the system auditor)

System Audit Report for the period _____ to _____)

I/We, M/s. _____ (Name of the system auditor / system audit firm) have conducted the follow-on system audit of Trading system facility/ies of the below mentioned trading member of National Stock Exchange for the observations about the non-compliance / non-conformities (NCs) made in the preliminary audit report. The summary of findings is reproduced below:

NSE Trading Member Code: _____

NSE Trading Member Name: _____

Preliminary Audit Date	S No.	Preliminary Observation Number	Preliminary Status	Preliminary Corrective Action	Current Finding	Current Status	Revised Corrective Action	Deadline for the Revised Corrective Action	Verified By	Closing Date

Declaration:

- All the branches/locations where the trading software facility is provided have been audited and ONE consolidated report has been submitted for all market segments.
- There is no conflict of interest with respect to the member being audited. If any such instance arises, it shall be brought to the notice of the Exchange immediately before undertaking the audit.
- With regard to the areas mentioned in the preliminary audit all observations specified as non-compliance status have been complied and met the requirement as specified in the Terms of Reference (TOR).

Signature

(Name of the Auditor & Auditing firm)
CISA / DISA / CISM / CISSP Reg. No. :

Date:

Place: Stamp / Seal

Description of relevant Table heads:

1. **Preliminary Status –** The original findings as per the preliminary system audit report
2. **Preliminary Corrective Action –** The original corrective action as prescribed in the preliminary system audit report
3. **Current findings –** The current findings w.r.t. the issue
4. **Current status –** Current status of the issue viz. (a) Non-Compliant (b) Complaint (c) Work In Progress
5. **Revised Corrective Action –** The revised corrective action prescribed w.r.t. the Non Compliance / WIP issues

Annexure - E
Terms of Reference (TOR) for System Audit

TOR Clause	Details		Applicability (NA= Not applicable ,Y=Applicable)		
		Mandatory/ Optional	Type I Broker	Type II Broker	Type III Broker
1.	**System Control and Capabilities**				
1(a)	**Order Tracking –** The system auditor should verify system process and controls at exchange provided terminals / NNF terminals (CTCL / IBT / DMA / SOR / STWT / ALGO) with regard to order entry, capturing of IP address of order entry terminals, modification / deletion of orders, status of the current order/outstanding orders and trade confirmation.	Mandatory	Y	Y	Y
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.	Mandatory	Y	Y	Y
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 / DMA / SOR / STWT / ALGO and at the servers of Exchange.	Mandatory	Y	Y	Y
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.	Mandatory	Y	Y	Y
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.	Mandatory	Y	Y	Y

1(f)	**Order type distinguishing capability** – Whether system has capability to distinguish the orders originating from CTCL / IBT/ DMA / STWT/SOR / ALGO. Whether CTCL / IBT / DMA / SOR / STWT / ALGO orders are having unique flag/ tag as specified by the Exchange and systems identify the orders emanating from CTCL / IBT / DMA / SOR / STWT / ALGO by populating the 15-digit NNF field in the order structure for every order. Whether Broker is using similar logic/ priorities as used by Exchange to treat CTCL / IBT / DMA / SOR / STWT client orders?	Mandatory	NA	Y	Y
1(g)	**The installed NNF system parameters are as per NSE norms:** CTCL / IBT / DMA / SOR / STWT / ALGO Version (as applicable) • 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)	Mandatory	NA	Y	Y
1(h)	**The installed system (viz. CTCL/ IBT / DMA / SOR / STWT system) features are as prescribed by the NSE.** 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	Optional	NA	Y	Y

	of trades for the day to the user				
1(i)	**The installed system (viz. CTCL/ IBT / DMA / SOR / STWT system) parameters are as per NSE norms** Gateway Parameters • Trader ID Market Segment - CM • CTCL ID • IP Address • (NSE Network) • VSAT ID • Leased Line ID Market Segment – F&O • CTCL ID • IP Address • (NSE Network) • VSAT ID • Leased Line ID Market Segment – CDS • CTCL ID • IP Address • (NSE Network) • VSAT ID • Leased Line ID	Optional	NA	Y	Y
1(j)	**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.	Optional	NA	Y	Y
1(k)	**Trades Information** **The installed NNF system provides a system based control facility over the trade confirmation process** Trade Confirmation and Reporting Feature	Optional	NA	Y	Y

	• 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				
2.	**Risk Management System (RMS)**				
2(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 exchange provided terminals / NNF terminals (CTCL / IBT/ DMA / SOR / STWT / ALGO)	Mandatory	Y	Y	Y
2(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.	Mandatory	Y	Y	Y
2(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.	Mandatory	Y	Y	Y
2(d)	**Order Review –**Whether the system has capability to facilitate review of such orders that were not validated by the system.	Mandatory	Y	Y	Y
2(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.	Mandatory	Y	Y	Y

2(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.	Mandatory	Y	Y	Y
2(g)	**Information Risk Management** Has the organization implemented a comprehensive integrated risk assessment, governance and management framework? Are Standards, Guidelines, templates, processes, catalogues, checklists, measurement metrics part of this Framework? Are the risk identification and assessment processes repeated periodically to review existing risks and identify new risks? Has the organization defined procedure/process for Risk Acceptance? Are reports and real time dashboards published in order to report/track Risks?	Mandatory	NA	Y	Y
2(h)	**Order Reconfirmation Facility** **The installed NNF 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	Mandatory	NA	Y	Y
2(i)	**Information Risk Management** Is there a dedicated Risk Management Team for managing Risk and Compliance activities? Are risks reported to the Senior Management through reports and dashboards on a periodic basis? Is the Risk Management Framework automated?	Optional	NA	Y	Y

	Are SLA's defined for all risk management activities? Has the organization developed detailed risk management program calendar to showcase risk management activities? If yes, is the risk management program calendar reviewed periodically?				
2(j)	**Settlement of Trades** **The installed NNF 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.	Optional	NA	Y	Y
3.	**Password Security**				
3(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 exchange provided terminals and for API based terminals (NNF terminals).	Mandatory	Y	Y	Y
3(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.	Mandatory	Y	Y	Y
3(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.	Mandatory	Y	Y	Y
3(d)	**The installed NNF system authentication mechanism is as per the guidelines of the NSE** The installed CTCL / IBT / DMA / SOR / STWT / ALGO	Mandatory	NA	Y	Y

	systems use passwords for authentication. The password policy / standard are documented. The system requests for identification and new password before login into the system. The installed system's Password features include • The Password is masked at the time of entry • System mandated changing of password when the user logs in for the first time • Automatic disablement of the user on entering erroneous password on three consecutive occasions • Automatic expiry of password on expiry of 14 calendar days for CTCL/DMA/SOR/ALGO systems • Automatic expiry of password on expiry of reasonable period of time as determined by member for IBT/STWT systems • System controls to ensure that the password is alphanumeric (preferably with one special character), instead of just being alphabets or just numerical • System controls to ensure that the changed password cannot be the same as of the last password • System controls to ensure that the Login id of the user and password should not be the same • System controls to ensure that the Password should be of minimum six characters and not more than twelve characters for CTCL / IBT / DMA / SOR / STWT .and minimum eight characters and not more than twelve characters for Algo . • System controls to ensure that the Password is encrypted at members end so that employees of the member cannot view the same at any point of time				
4.	**Session Management**				
4(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	Mandatory	Y	Y	Y

	authentication mechanisms like SSL etc.				
4(b)	**Session Security** – Whether there is availability of an end-to-end encryption for all data exchanged between client and broker systems or other means of ensuring session security. Whether session login details are stored on the devices used for IBT and STWT.	Mandatory	Y	Y	Y
4(c)	**Inactive Session** – Whether the system allows for automatic trading session logout after a system defined period of inactivity.	Mandatory	Y	Y	Y
4(d)	**Log Management** – Whether the system generates and maintain logs of Number of users, activity logs, system logs, Number of active clients.	Mandatory	Y	Y	Y
4(e)	**Cryptographic Controls :** Does the organization have a documented process/framework for implementing cryptographic controls in order to protect confidentiality and integrity of sensitive information during transmission and while at rest, using suitable encryption technology? Is the encryption methodology of information involved in business transactions based on Regulation/Law/Standards compliance requirements? Does the organization ensure Session Encryption for internet based applications including the following? Do the systems use SSL or similar session confidentiality protection mechanisms? Do the systems use a secure storage mechanism for storing of usernames and passwords? Do the systems adequately protect the confidentiality of the users' trade data? Does the organization ensure that the data transferred through internet is protected with suitable encryption technologies? Are transactions on the website suitably encrypted?	Mandatory	NA	Y	Y

4(f)	**Cryptographic Controls** Is Secret and confidential information sent through e-mails encrypted before sending? Is Secret and confidential data stored in an encrypted format?	Optional	NA	Y	Y
5.	**Network Integrity**				
5(a)	**Seamless connectivity** – Whether stock broker has ensured that a backup network link is available in case of primary link failure with the exchange.	Mandatory	Y	Y	Y
5(b)	**Network Architecture** – Whether the web server is separate from the Application and Database Server.	Mandatory	Y	Y	Y
5(c)	**Firewall Configuration** – Whether appropriate firewall is present between stock broker's trading setup and various communication links to the exchange. Whether the firewall is appropriately configured to ensure maximum security.	Mandatory	Y	Y	Y
5(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?	Mandatory	NA	Y	Y

	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?				
6.	**Access Controls**				
6(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.	Mandatory	Y	Y	Y
6(b)	**Additional Access controls** – Whether the system provides for any authentication/two factor authentication mechanism to access to various components of the exchange provided terminals / NNF terminals (CTCL / IBT/ DMA / SOR / STWT / ALGO)respectively. Whether additional password requirements are set for critical features of the system. Whether the access control is adequate.	Mandatory	Y	Y	Y
6(c)	**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	Mandatory	NA	Y	Y

	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?				
6(d)	**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,	Mandatory	NA	Y	Y

	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?				
6(e)	**Privileged Identity Management** Does the organization have a documented process/procedure for defining reviewing and assigning the administrative roles and privileges? Has the organization implemented controls/tools for Privilege Identity Management including at a minimum provisioning, maintenance, monitoring, auditing and reporting all the activities performed by privileged users (Sys Admin, DBA etc.) accessing organization's IT systems? Are Privileges granted to users based on appropriate approvals and in accordance with the user's role and responsibilities? Are all the activities of the privileged users logged? Are log reviews of privileged user logs of admin activity conducted periodically? Is Maker- Checker functionality implemented for all changes by admin? Are records of privileged user provisioning/de-provisioning reviewed?	Mandatory	NA	Y	Y
6(f)	**Extra Authentication Security** The systems uses additional authentication measures like	Optional	NA	Y	Y

	smart cards, biometric authentication or tokens etc.				
7.	**Backup and Recovery**				
7(a)	**Backup and Recovery Policy** – Whether the organization has a well documented policy on periodic backup of data generated from the broking operations.	Mandatory	Y	Y	Y
7(b)	**Log generation and data consistency -** Whether backup logs are maintained and backup data is tested for consistency.	Mandatory	Y	Y	Y
7(c)	**System Redundancy** – Whether there are appropriate backups in case of failures of any critical system components.	Mandatory	Y	Y	Y
7(d)	**Backup & Restoration** Does the organization documented policy & procedures include process/policy for Backup and restoration in order to ensure availability of information? Are backups of the following system generated files maintained as per the NSE guidelines? At server/gateway level • Database • Audit Trails • Reports At the user level • Logs • History • Reports • Audit Trails • Alert logs • Market Watch Does the organization ensure that the user details including user name, unique identification of user, authorization levels for the users activated for algorithm facilities maintained and is available for a minimum period of 5 years? Does the audit trail capture the record of control	Mandatory	NA	Y	Y

	parameters, orders, trades and data points emanating from trades executed through algorithm trading? Does the organization ensure that the audit trail data maintained is available for a minimum period of 5 years? Does the audit trail for SOR capture the record of orders, trades and data points for the basis of routing decision? Are backup procedures documented? Have backups been verified and tested? Are back up logs maintained? Are the backup media stored safely in line with the risk involved? Are there any recovery procedures and have the same been tested? Are the backups restored and tested periodically to ensure adequacy of backup process and successful restoration?				
7(e)	**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 NSE? • Is the backup network link adequate in case of failure of the primary link connecting the users? • Is there an alternate communications path between customers and the firm? • Is there e an alternate communications path between the firm and its employees? • Is there an alternate communications path with critical business constituents, banks and regulators?	Mandatory	NA	Y	Y
7(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**	Optional	NA	Y	Y

	System Failure Backup Are there suitable backups for failure of any of the critical system components like • Gateway / Database Server • Router • Network Switch Infrastructure breakdown backup Are there suitable arrangements made for the breakdown in any infrastructure components like • Electricity • Water • Air Conditioning Primary Site Unavailability Have any provision for alternate physical location of employees been made in case of non-availability of the primary site Disaster Recovery Are there suitable provisions for Books and records backup and recovery (hard copy and electronic). Have all mission-critical systems been identified and provision for backup for such systems been made?				
8.	**BCP/DR (Only applicable for Stock Brokers having BCP / DR site)**				
8(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 procedures.	Mandatory	Y	Y	Y
8(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).	Mandatory	Y	Y	Y
8(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.	Mandatory	Y	Y	Y

8(d)	**Connectivity with other FMIs** – The system auditor should check whether there is an alternative medium to communicate with Stock Exchanges and other FMIs.	Mandatory	Y	Y	Y
8(e)	**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?	Mandatory	NA	Y	Y
8 (f)	**Security Incident & Event Management** Is there a dedicated Incident Response Team for managing risk and compliance activities?	Optional	NA	Y	Y
8(g)	**Business Continuity** Does the organization have a documented process / framework to ensure the continuation and/or rapid recovery from failure or interruption of business and Information Technology processes and systems? Does the organization maintain a Business Continuity Plan? Does the organization conduct periodic redundancy/	Mandatory	NA	Y	Y

	contingency testing? Are BCP drills performed periodically? Is the defined framework/process updated and reviewed periodically?				
8(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?	Optional	NA	Y	Y
9.	**Segregation of Data and Processing facilities**				
9(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.	Mandatory	Y	Y	Y
10.	**Back office data**				
10(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.	Mandatory	Y	Y	Y
10(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.	Mandatory	Y	Y	Y
11.	**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))**				

11(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.	Mandatory	Y	Y	Y
11(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.	Mandatory	Y	Y	Y
11(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	Mandatory	Y	Y	Y
11(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.	Mandatory	Y	Y	Y
11(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?	Mandatory	NA	Y	Y
11(f)	**Standards & Guidelines**	Mandatory	NA	Y	Y

	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?				
11 (g)	**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?	Mandatory	NA	Y	Y
11(h)	**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?	Optional	NA	Y	Y
11(i)	**To ensure information security for the Organization in general and the installed system in particular policy and procedures as per the NSE 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 NSE requirements and whether they	Optional	NA	Y	Y

	have been implemented by the organization? • Information Security Policy • Password Policy • User Management and Access Control Policy • Network Security Policy • Application Software Policy • Change Management Policy • Backup Policy • BCP and Response Management Policy • Audit Trail Policy • Capacity Management Plan Does the organization follow any other policy or procedures or documented practices that are relevant?				
11(j)	**Are documented practices available for various system processes** • Day Begin • Day End • Other system processes • Audit Trails • Access Logs • Transaction Logs • Backup Logs • Alert Logs • Activity Logs • Retention Period • Misc.	Optional	NA	Y	Y
11(k)	**Is a log of success / failure of the process maintained?** Day Begin Day End Other system processes	Optional	NA	Y	Y
11(l)	**In case of failure, is there an escalation procedure implemented?** • Details of the various response procedures incl. for • Access Control failure • Day Begin failure • Day End failure • Other system Processes failure	Optional	NA	Y	Y
11(m)	**Vulnerability Assessment, Penetration Testing & Application Security Assessments**:	Mandatory	NA	Y	Y

	Does the organization have documented processes/procedures for conducting vulnerability assessments, penetration tests and application security assessments? Are these assessments conducted periodically in order to proactively identify threats and vulnerabilities arising from both internal and external sources in order to maintain a strong security posture? **Vulnerability Assessment (VA)** Are periodic vulnerability assessments for all the assets including Servers, OS, Database, Middleware, Network Devices, Firewalls, IDS /IPS etc conducted? Is Firewall Rule base and IDS/IPS Policy reviews taken up as a part of Vulnerability Assessment? **Penetration Testing (PT)** Are periodic Penetration Tests conducted? Application Security Assessment (AppSec) Are periodic application security assessments conducted? Are reports published for the findings of Vulnerability Assessment/Penetration Testing's/Application Security Assessments? Are findings of Vulnerability Assessment / Penetration Testing's / Application Security Assessments reviewed and tracked to closure?				
11(n)	**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	Mandatory	NA	Y	Y

	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?				
11(o)	**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?	Optional	NA	Y	Y
12.	**Software Change Management - The system auditor should check whether proper procedures have been followed and proper documentation has been maintained for the following:**				
12(a)	Processing / approval methodology of new feature request or patches	Mandatory	NA	Y	Y
12(b)	Fault reporting / tracking mechanism and process for resolution	Mandatory	NA	Y	Y
12(c)	Testing of new releases / patches / modified software / bug fixes	Mandatory	NA	Y	Y
12(d)	Version control- History, Change Management process , approval etc	Mandatory	NA	Y	Y
12(e)	Development / Test / Production environment segregation.	Mandatory	NA	Y	Y
12(f)	New release in production – promotion, release note approvals	Mandatory	NA	Y	Y
12(g)	Production issues / disruptions reported during last year, reasons for such disruptions and corrective actions taken.	Mandatory	NA	Y	Y

12(h)	User Awareness	Mandatory	NA	Y	Y
12(i)	The system auditor should check whether critical changes made to the CTCL / IBT / DMA / STWT/ SOR / ALGO are well documented and communicated to the Stock Exchange.	Mandatory	NA	Y	Y
12(j)	**Change Management** Has the organization implemented a change management process to avoid risks due to unplanned and unauthorized changes for all the information security assets (Hardware, software, networks, applications)? Does the process at a minimum include the following? • Planned Changes Are changes to the installed system made in a planned manner? Are they made by duly authorized personnel? • Risk Evaluation Process Is the risk involved in the implementation of the changes duly factored in? • Change Approval Is the implemented change duly approved and process documented? • Pre-implementation process Is the change request process documented? • Change implementation process Is the change implementation process supervised to ensure system integrity and continuity • Post implementation process. Is user acceptance of the change documented? • Unplanned Changes In case of unplanned changes, are the same duly authorized and the manner of change documented later? • Are Records of all change requests maintained?Are periodic reviews conducted for all the changes which were implemented?	Mandatory	NA	Y	Y
12(k)	**Patch Management**	Mandatory	NA	Y	Y

	Does the organization have a documented process/procedure for timely deployment of patches for mitigating identified vulnerabilities? Does the organization periodically update all assets including Servers, OS, Database, Middleware, Network Devices, Firewalls, IDS /IPS Desktops etc. with latest applicable versions and patches?				
12(l)	**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?	Mandatory	NA	Y	Y
12(m)	**SDLC - Application Development & Maintenance** In case of members self-developed system SDLC documentation and procedures if the installed system is developed in-house.	Optional	NA	Y	Y
12(n)	**Human Resources Security, Acceptable Usage & Awareness Trainings** Are periodic surprise audits and social engineering attacks conducted to assess security awareness of employees and vendors?	Optional	NA	Y	Y

13.	**Smart order routing (SOR) - The system auditor should check whether proper procedures have been followed and proper documentation has been maintained for the following:**				
13(a)	**Best Execution Policy** – System adheres to the Best Execution Policy while routing the orders to the exchange.	Mandatory	NA	Y	Y
13(b)	**Destination Neutral** – The system routes orders to the recognized stock exchanges in a neutral manner.	Mandatory	NA	Y	Y
13(c)	**Class Neutral** – The system provides for SOR for all classes of investors.	Mandatory	NA	Y	Y
13(d)	**Confidentiality** - The system does not release orders to venues other than the recognized stock Exchange.	Mandatory	NA	Y	Y
13(e)	**Opt–out** – The system provides functionality to the client who has availed of the SOR facility, to specify for individual orders for which the clients do not want to route order using SOR.	Mandatory	NA	Y	Y
13(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.	Mandatory	NA	Y	Y
13(g)	**Audit Trail** - Audit trail for SOR should capture order details, trades and data points used as a basis for routing decision.	Mandatory	NA	Y	Y
13(h)	**Server Location** - The system auditor should check whether the order routing server is located in India	Mandatory	NA	Y	Y
13(i)	**Alternate Mode** - The system auditor should check whether an alternative mode of trading is available in case of failure of SOR Facility	Mandatory	NA	Y	Y
14.	**Database Security**				
14(a)	**Access** – Whether the system allows NNF - database access only to authorized users / applications.	Mandatory	NA	Y	Y

14(b)	**Controls** – Whether the NNF database server is hosted on a secure platform, with Username and password stored in an encrypted form using strong encryption algorithms.	Mandatory	NA	Y	Y
15.	**User Management**				
15(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.	Mandatory	NA	Y	Y
15(b)	**Access to Authorized users** – The system auditor should check whether the system allows access only to the authorized users of the NNF 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.	Mandatory	NA	Y	Y
15(c)	**User Creation / Deletion** – The system auditor should check whether new users ids were created / deleted as per NNF guidelines of the exchange and whether the user ids are unique in nature.	Mandatory	NA	Y	Y
15(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.	Mandatory	NA	Y	Y
15(e)	**User Management system:** Reissue of User Ids: User Ids are reissued as per the NSE guidelines. Locked User Accounts: Users whose accounts are locked are unlocked only after documented unlocking requests are made.	Mandatory	NA	Y	Y
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.	Mandatory	NA	Y	Y
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.	Mandatory	NA	Y	Y
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.	Mandatory	NA	Y	Y
17.	**Algorithmic Trading - The system auditor should check whether proper procedures have been followed and proper documentation has been maintained for the following:**				
17(a)	**Change Management** –Whether any changes (modification/addition) to the approved algos were informed to and approved by stock exchange. The inclusion / removal of different versions of algos should be well documented.	Mandatory	NA	NA	Y
17(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 orders through Algorithmic trading. The system has functionality for mandatorily routing of orders generated by algorithm through the automated risk management system and only those orders that are within the parameters specified in the risk management systems are allowed to be released to exchange trading system. The risk management system has following minimum levels of risk controls functionality and only algorithm	Mandatory	NA	NA	Y

	orders that are within the parameters specified by the risk management systems are allowed to be placed. A) Individual Order Level: • Quantity Limits • Price Range checks • Trade price protection checks • Order Value Checks (Order should not exceed the limit specified by the Exchange) • Market price protection • Spread order Quantity and Value Limit B) Client Level: • Cumulative Open Order Value check • Automated Execution check • Net position v/s available margins • RBI violation checks for FII restricted stocks • Market-wide Position Limits (MWPL) violation checks • Position limit checks • Trading limit checks • Exposure limit checks at individual client level and at overall level for all clients • 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)				
17(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.	Mandatory	NA	NA	Y
17(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	Mandatory	NA	NA	Y

	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.				
17(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.	Mandatory	NA	NA	Y
17(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.	Mandatory	NA	NA	Y
17(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.	Mandatory	NA	NA	Y

	v. Whether the system captures the IP address from where the algo orders are originating.				
17(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?	Mandatory	NA	NA	Y
17(i)	**Reporting to Stock Exchanges** – The system auditor should check whether the stock broker is informing the stock exchange regarding any incidents where the algos have not behaved as expected. The system auditor should also comment upon the time taken by the stock broker to inform the stock exchanges regarding such incidents.	Mandatory	NA	NA	Y
17(j)	**Mock Testing:** Have all user-ids approved for Algo trading, irrespective of the algorithm having undergone change or not, participated in the mock trading sessions minimum once a month?	Mandatory	NA	NA	Y
18.	**Additional Points**				

18(a)	**Vendor Certified Network diagram** Date of submission of network diagram to NSE(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	Mandatory	NA	Y	Y
18(b)	**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?	Mandatory	NA	Y	Y
18(c)	**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	Optional	NA	Y	Y
18(d)	**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	Mandatory	NA	Y	Y

	licensing requirements and asset inventory?				
18(e)	**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 & Malwareattacks? Does the organization have a process for tracking down phishing sites?	Mandatory	NA	Y	Y
18(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 NNF user ids created in the server of the trading member, for any purpose (viz. administration, branch administration, mini-	Mandatory	NA	Y	Y

	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 NNF 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 NNF 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 NNF field is populated with 0. All orders routed through CTCL / IBT / STWT / DMA / SOR are routed through electronic / automated Risk Management System of the broker to carry out appropriate validations of all risk parameters before the orders are released to the Exchange. The system and system records with respect to Risk Controls are maintained as prescribed by the Exchange which are as follows : • The limits are setup after assessing the risks of the 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				

18(g)	**DOS** Has the organization implemented strong monitoring, logging, detection and analysis capability to detect and mitigate DOS/DDOS attacks? Does the organization have a documented process/procedure/policy defining roles and responsibilities and plan of action in order to deal with DOS/DDOS attacks pro-actively and post the incidence? Does the organization collaborate with ISP's for tackling DOS/DDOS attacks?	Mandatory	NA	Y	Y
18(h)	**DOS** Does the organization periodically conducts mock DOS scenarios to have insight into the preparedness in tackling with DOS/DDOS attacks?	Optional	NA	Y	Y
18(i)	**Human Resources Security, Acceptable Usage & Awareness Trainings** Has the organization implemented policy/procedure defining appropriate use of information assets provided to employees and vendors in order to protect these assets from inappropriate use? Are these policies/procedures periodically updated? Does the organization perform Background Checks for employees (permanent, temporary) before employment? Does the organization conduct Information Security Awareness Program through trainings and Quiz for employees and vendors?	Mandatory	NA	Y	Y
18(j)	**Independent Audits** Are periodic independent audits conducted by Third Party / internal Auditors?	Mandatory	NA	Y	Y

	Are the audit findings tracked to closure?				
18(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?	Mandatory	NA	Y	Y
18(l)	**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?	Mandatory	NA	Y	Y
18(m)	**Event Logging and System Monitoring** The installed NNF systems provides a system based event logging and system monitoring facility which monitors and logs all activities / events arising from actions taken on the gateway / database server, authorized user terminal and transactions processed for clients or otherwise and the same is not susceptible to manipulation. The installed CTCL / IBT / DMA / SOR / STWT systems has a provision for On-line surveillance and risk management as per the requirements of NSE and includes • Number of Users Logged in / hooked on to the network incl. privileges of each	Mandatory	NA	Y	Y

	The installed CTCL / IBT / DMA / SOR / STWT systems has a provision for off line monitoring and risk management as per the requirements of NSE and includes reports / logs on • Number of Authorized Users • Activity logs • Systems logs • Number of active clients				
18(n)	**Compliance of NSE Circulars** **The system has been installed after complying with the various NSE circulars** 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, if any.	Optional	NA	Y	Y
18(o)	**Insurance** The insurance policy of the Member covers the additional risk of usage of CTCL/IBT/STWT/SOR/DMA/ALGO as applicable.	Optional	NA	Y	Y
18(p)	**Firewall** Is a firewall implemented? Are the rules defined in the firewall adequate to prevent unauthorized access to IBT/DMA/STWT systems	Optional	NA	Y	Y