Circular No.: MCX/TECH/676/2024 October 09, 2024

System Audit of Trading Member - ATF Members (Type III)

In terms of provisions of the Rules, Bye-Laws and Business Rules of the Exchange and in continuation to SEBI circular no. CIR/MRD/DMS/34/2013 dated November 6, 2013 and the Exchange circular no. MCX/CTCL/423/2017 dated November 15, 2017, the Exchange circular no. MCX/CTCL/213/2023 dated March 31, 2023 on Uniform Terms of Reference for System Audit, the Exchange Master circulars ref. no. MCX/TECH/444/2023 dated June 30, 2023 and MCX/TECH/280/2024 dated April 30, 2024, members are required to submit system audit report as per the norms specified therein.

As per the provision of Master Circular, Trading Members are required to undertake system audit of their software for the period through System Auditor as per Auditor Selection Norms and submit the System Audit Report (SAR) to the Exchange within the timeline as mentioned in the table below:

Periodicity of Audit	Criteria	Type of Broker	Due Date for Submission of Reports	
			Audit Report	Action Taken Report, if applicable
Half Yearly (April 2024 – September 2024)	Members using ATF facility and QSB	Type of Broker-III	November 30, 2024	February 28, 2025

Members are required to submit the System Audit Report online through Member Portal - https://member.mcxindia.com and same shall be made available for submission from **October 18, 2024**. Terms of Reference (ToR) are incorporated in the online Member portal and **'System Audit Report – Help File'** is available on the portal and on shared path https://sftp.mcxindia.com/Common/Online portal help files folder.

Additionally, auditor will also be provided details of vendor/in-house developed products & application being used and registered with Exchange by trading member. The system auditor shall confirm whether the trading member has deployed the latest version in live environment and provide its version number being used for each product in auditor submission login. The system audit report can be submitted only after submission of version confirmation.

---------- Corporate office ----------
Multi Commodity Exchange of India Limited
Exchange Square, CTS 255, Suren Road, Chakala, Andheri (East), Mumbai – 400 093
Tel.: 022 – 6649 4000 Fax: 022 – 6649 4151 www.mcxindia.com
email: customersupport@mcxindia.com

The online SAR portal will be available only to the applicable Members for audit report submission as per the schedule specified below:

Periodicity of System Audit	Report Submission Period
Type of Broker – III	Half Yearly (April 2024 – September 2024)

Trading members are requested to take note that, for each non-compliance reported by auditor, trading members are required to submit corrective action taken report as per above mentioned timelines. Further, based on audit findings and related risks it should indicate if a follow-on audit is required to review the status of NCs (non-compliances). In order to ensure that the timely corrective actions are taken by the Trading members, follow-on audit, if any, shall be scheduled by the trading member as per above mentioned timelines.

Submission of System Audit Report with Management comments shall be considered complete only after Member submits the report to the Exchange and receives an acknowledgment email. Saved reports/reports submitted by auditor will not be considered as final submission. Further, auditor has to provide compliance status for each TOR item i.e., **Compliant/Non-Compliant and Not Applicable** and in case of any TOR item which is not applicable, auditor is required to provide justification for the non-applicability of said TOR.

Members are requested to refer to the below mentioned documents while submitting the system audit report.

- Details of Auditor – **Annexure I**
- Auditor Selection Norms – **Annexure II**
- Terms of Reference (ToR for type II and Type III) – **Annexure III**

Trading Members are requested to take note of the Exchange circular MCX/TECH/856/2023 dated December 11, 2023, regarding "Revised Penalties/disciplinary action(s)/charges for System Audit Report and Cyber Security & Cyber Resilience Audit Report related submissions".

Members are requested to note the list of System Auditors registered by Members earlier is available in the above-mentioned portal. Kindly submit attached Annexure 1 (E-Mail to Reporting@mcxindia.com) to update the Auditor details which are not reflecting in online SAR portal of Exchange.

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

For and on behalf of
Multi Commodity Exchange of India Ltd.

Abhay Angarkar
VP – Technology

Annexure 1

Details of Auditor

Particulars	**Details**
Name of Auditor	
Auditor Membership No	
Auditor Firm Name	
Email Address	
Auditor Firm Registration No.	
Registered Address	
Contact number	
Auditor Qualification CISA / DISA / CISM / CISSP	
Certification Number	
Regulatory Action against Auditor / Partner / Director	(Yes / No)

Annexure II

Auditor Selection Norms:

1. The Auditor should have experience of IT audit/governance frameworks and processes conforming to industry leading practices like COBIT 5/ISO 27001.

2. The Auditor shall have a minimum of 3 years of experience in IT audit of securities market participants e.g., Stock Exchanges, Clearing Corporations, Depositories, Trading Member, 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.

3. The Auditor/Auditor firm can perform a maximum of 3 successive audits of the Trading Member. Follow-on audit conducted by the auditor shall not be considered in the successive audits. However, such an auditor shall be eligible for re-appointment after a cooling-off period of one year.

4. Resources employed for the purpose of system audit should possess at least one of the following certifications:

- CISA (Certified Information System Auditors) from ISACA
- DISA (Post Qualification Certification in Information Systems Audit) from Institute of Chartered Accountants of India (ICAI)
- CISM (Certified Information Security Manager) from ISACA
- CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium, commonly known as (ISC)2.

5. The Auditor, as being appointed by Trading Member must not have any conflict of interest in conducting fair, objective, and independent audit. Further, the directors / partners of Audit firm shall not be related to any Directors/Promoters/Proprietor of the said Trading Members either directly or indirectly.

6. Auditor should not have been engaged over the last three years in any consulting engagement with any departments / units of the Trading Member.

7. 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.

8. The trading members and auditors are required to retain records of physical visits conducted during audits like name, qualification & date of visit/s of auditor, along with audit artifacts, proofs of concept (POCs), and evidence related to terms of reference (TOR) points for a minimum duration of three years.

System Audit - Terms of Reference (TOR) - Annexure III

(Members using CTCL Facility)

Audit TOR Clause	Details
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.
1(b)	Order Status/ Capture – Whether the system has capability to generate / capture order id, time stamping, order type, scrip details, action, quantity, price and validity etc.
1(c)	Rejection of orders – Whether system has capability to reject orders which do not go through order level validation at the end of the stock broker CTCL / IBT / SOR/ STWT / ALGO / DMA etc. and at the servers of Exchange.
1(d)	Communication of Trade Confirmation / Order Status – Whether the system has capability to timely communicate to Client regarding the Acceptance/ Rejection of an Order / Trade via various media including e-mail; facility of viewing trade log.
1(e)	Client ID Verification – Whether the system has capability to recognize only authorized Client Orders and mapping of Specific user Ids to specific predefined location for proprietary orders. - Whether System has settings to restrict / allow the facility to place orders in pro account from a CTCL Terminal. - Whether there is a proper process for enabling the facility of placing orders in pro account from the Exchange approved location through a CTCL terminal.
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.
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).
1(h)	The installed system (viz. CTCL/ IBT / STWT / SOR / DMA/SOR system) features are as prescribed by the Exchange. Main Features: (1) Price Broadcast The system has a feature for receipt of price broadcast data.

	(2) Order Processing: The system has a feature : • Which allows order entry and confirmation of orders • which allows for modification or cancellation of orders placed. (3) 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.
1(i)	Execution of Orders / Order Logic 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.
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

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.
1(l)	System Auditor to check whether DMA facility has been offered to only those categories of investors which have been permitted by the Stock Exchange. System Auditor to Refer Clause 2.2.3.1. Chapter 2 of SEBI master circular SEBI/HO/MRD2/PoD-2/CIR/P/2023/171 dated October 16, 2023, and point no. 5. of chapter 12 from MCX master circular MCX/CTCL/281/2024 dated April 30, 2024.
1(m)	System Auditor to check whether Stock Broker has system / policy in place to ensure that only clients who fulfil the eligibility criteria are permitted to use the DMA facility. System Auditor to Refer Clause 2.2.6.1. Chapter 2 of SEBI master circular SEBI/HO/MRD2/PoD-2/CIR/P/2023/171 dated October 16, 2023.
1(n)	System Auditor to check whether the software (CTCL/IBT/STWT/DMA/Algo etc.) which are obsolete, not in use, software running on old versions, unsupported software etc. has been discontinued & decommissioned from environment by trading member and they have complied with the Exchange Cir. No. MCX/CTCL/281/2024 dated April 30, 2024.
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
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?
2(c)	Fault reporting / tracking mechanism and process for resolution
2(d)	Testing of new releases / patches / modified software / bug fixes Does demonstratable segregation exists between Development / Test / Production environment
2(e)	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.
2(f)	New release in production – promotion, release note approvals
2(g)	Production issues / disruptions reported during last year, reasons for such disruptions and corrective actions taken.
2(h)	User Awareness
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.

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?
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?
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.
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?
2(n)	Changes undertaken pursuant to a change to the stock Exchanges trading system.
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.
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 / STWT / ALGO / SOR).
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.
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.
3(d)	Order Review –Whether the system has capability to facilitate review of such orders that were not validated by the system.
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.
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.
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
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.

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?
3(j)	Has the organization deployed alert mechanism for detecting malfunctioning of device, software and backup system?
3(k)	All member should have system in place to calculate all obligations of client such as margin obligation/ client position etc. during the day on the basis of various files (trade files, margin parameters file and settlement price file) being provided by Clearing Corporation/Exchange.
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.
4(b)(a)	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 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.
4(b)(a)(i)	A) Individual Order Level: • Quantity Limits / Maximum Order Size

4(b)(a)(ii)	• Daily Price Range checks
4(b)(a)(iii)	• Trade price protection checks - Orders shall not be released in breach of the bad trade price for the security in respective segment. System Auditor shall refer relevant MCX circulars with respect to “Pre-Trade risk controls - Market Price Protection” and “Pre-Trade risk controls - Limit Price Protection”. System auditor shall verify these checks which are designed to reduce excessive order rejections due to LPP and normally order placement is within the ranges as prescribed by Exchange circulars.
4(b)(a)(iv)	• Order Value Checks (Order should not exceed the limit specified by the Exchange) The order value check should be within the ranges as prescribed by Exchange circulars.
4(b)(a)(v)	• Market price protection (the pre-set percentage of LTP shall necessarily be accompanied by a limit price) Members are required to adhere to the Market Price Protection check, by not placing any algorithmic orders on the Exchange as a market order. System Auditor shall refer relevant MCX market operation master circulars with respect to “Pre-Trade risk controls - Market Price Protection”. System auditor shall verify these checks which are designed to ensure that order placement is within the ranges as prescribed by Exchange circulars
4(b)(a)(vi)	• Spread order Quantity and Value Limit
4(b)(a)(vii)	• For all checks in Individual Order Level, Trading Members (TM) are required to maintain a policy which shall be approved by the Board/All partners/Proprietor of the Trading Member.
4(b)(b)(i)	B) Client Level: • Cumulative Open Order Value check
4(b)(b)(ii)	• Automated Execution check
4(b)(b)(iii)	• Net position v/s available margins
4(b)(b)(iv)	• Market-wide Position Limits (MWPL) violation checks
4(b)(b)(v)	• Position limit checks
4(b)(b)(vi)	• Trading limit checks
4(b)(b)(vii)	• Exposure limit checks at individual client level and at overall level for all clients
4(b)(b)(viii)	• Branch value limit for each branch ID
4(b)(b)(ix)	• Security wise limit for each user ID
4(b)(b)(x)	• Identifying dysfunctional algorithms
4(b)(b)(xi)	Does system has functionality to specify values as unlimited for any risk controls listed above?
4(b)(b)(a)(i)	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
4(b)(b)(a)(ii)	As a part of the 13 checks mentioned in the MCX operation master circular, Exchange would like to reiterate trading members should adhere to the Market Price Protection check, by not placing any algorithmic orders on the Exchange as a market order.
4(b)(b)(a)(iii)	• 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. In case any NNF ID not tagged as Algo and is sending excessive order messages the same should also be checked and validated. System Auditor should check whether NNF IDs are properly tagged or not.

4(c)(i)	Risk Parameters Controls – The system should allow only authorized person to set the risk parameter. The system auditor should verify the process for any change in Risk Parameters and check whether changes are being done only by Authorised person with proper validation/re-confirmation.
4(c)(ii)	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. System auditor should verify & conduct audit of logs maintained for all modifications in Risk Parameters.
4(c)(iii)	For Risk Parameters Controls Trading Members (TM) are required to maintain a policy along with authorisation for any change, validation/modification by authorised person. The said policy shall be approved by the Board/All partners/Proprietor of the Trading Member.
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.
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
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
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.

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?
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)
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?
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
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

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?
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
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
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).
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.
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.
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.
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.
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.
6(c)	Inactive Session – Whether the system allows for automatic trading session logout after a system defined period of inactivity.
6(d)	Log Management – Whether the system generates and maintain logs of Number of users, activity logs, system logs, Number of active clients.
6(e)	The installed system has provision for security, reliability and confidentiality of data through use of encryption technology. 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.

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?
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?
6(h)	Does the organization have deployed data loss prevention (DLP)solutions / processes?
7	**Database Security**
7(a)	Access – Whether the system allows CTCL - database access only to authorized users / applications.
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.
7(c)	Data at rest is encrypted
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.
8(b)	Network Architecture – Whether the web server is separate from the Application and Database Server.
8(c)	Firewall Configuration – Whether appropriate firewall is present between stock brokers 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
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

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.
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/ WT / ALGO)respectively. Whether additional password requirements are set for critical features of the system. Whether the access control is adequate.
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?
9(d)	Extra Authentication Security If the systems uses additional authentication measures like smart cards, biometric authentication or tokens etc.
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?
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?
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.
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.
10(b)	Log generation and data consistency - Whether backup logs are maintained and backup data is tested for consistency.
10(c)	System Redundancy – Whether there are appropriate backups in case of failures of any critical system components.

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?
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?

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.
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?

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 and observation on the DR drills conducted by the stock broker. Further, the system auditor should verify whether DR Drills were conducted on Trading day and whether all the clients were shifted to the DR site during the drill
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).
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.
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.
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?
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?
11(g)	Security Incident & Event Management Is there a dedicated Incident Response Team for managing risk and compliance activities?
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?

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.
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?
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.
12(b)	System Auditor to check where the Trading Member having more than one broking entity within a group or having common Promoters or where both Holding/subsidiary entities are registered as Trading Member has maintained appropriate segregation of infrastructure and data to uphold confidentiality.
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.
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.
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.
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.
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.

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.
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
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.
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.
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.
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.
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?

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?
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
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
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?

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?
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?
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?
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?
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?
15(o)	Does the organisation have hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments.
15(p)	Amazons 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?
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. ?
15(r)	Does the organisation implement appropriate security measures for production, 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?
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?
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.
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 organizations standards.
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.
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?
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
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
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
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

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 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
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?
17(i)	DOS Does the organization periodically conduct mock DOS scenarios to have insight into the preparedness in tackling with DOS/DDOS attacks?
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?
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? System auditor shall verify whether the member has put in place, a mechanism to handle increase in capacity in proportion to the increase in client base/financial turnover. • Whether peak load is monitored for all critical systems and alerts generated on threshold reaching 70% of capacity
17(l)	Independent Audits Are periodic independent audits conducted by Third Party / internal Auditors? Are the audit findings tracked to closure?

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?
17(n)	Does the organization display the 'Risk disclosures' given at Annexure-I Circular no SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/73 dated May 19, 2023 on their websites and to all their clients in the manner as specified below: 1. Upon login into their trading accounts with brokers, the clients may be prompted to read the 'Risk disclosures' (which may appear as a pop-up window upon login) and shall be allowed to proceed ahead only after acknowledging the same. 2. The 'Risk disclosures' shall be displayed prominently, covering at least 50 percent area of the screen.
17(o)	Whether a functionality is developed on stock broker's (with retail clients) non-NEAT front end including IBT,STWT,CTCL etc whereby any person placing an order in a security which is under Graded Surveillance Measure(GSM)/ Additional Surveillance Measure(ASM)/IRP as per IBC/Unsolicited SMS or Videos/Pledge/ASM ICA/ASM IBC etc gets the message as per the time of placing the order and is aware of such surveillance action on the scrip before placing the order. **(Not applicable for commodity Exchange)**
17(p)	Compliance with Exchange circular Whether the Member has developed the functionality to facilitate dissemination of scrip specific cautionary messages (single/multiple) on trading terminals at the time of order entry (for Buy & Sell both) to identify securities which are under Surveillance and Other actions, on their nonNEAT front end including IBT, STWT, CTCL etc., as per Exchange Circular Whether any person(client of the Member) while placing an order in a security for which the cautionary indicators are applicable (as per the REG_INDDDMMYY.csv file and 'fo_secban_DDMMYYYY.csv'), gets the following message so that the person placing the order is aware of such single/multiple actions on the scrip before placing the order. In case multiple messages are eligible to be displayed, whether trading members are providing all eligible messages in the pop-up. Whether the Member has included the verbatim of the pop-up message on the trading front-end. **(Not applicable for commodity Exchange)**
17(q)	Whether the member is complying with the Exchange circular MCX/CTCL/748/2022 dated December 29, 2022 for "Display of Brokerage, Statutory & Regulatory Levies"
17(r)	Whether member is allowing to place orders to only approved FPI clients using DMA facility as specified in as per SEBI/HO/MRD/MRD-RAC-1/P/CIR/2022/131 September 29, 2022 regarding Participation of SEBI registered Foreign Portfolio Investors(FPIs)in Exchange Traded Commodity Derivatives in India and SEBI circular i.e. SEBI/HO/MRD/MRD-PoD-1/P/CIR/2023/68 May 10, 2023 regarding "Direct Market Access(DMA)to

	SEBI registered Foreign Portfolio Investors (FPIs) for participating in Exchange Traded Commodity Derivatives(ETCDs)"
17(s)	Change Management: (Applicable to COLO Members) **(Not applicable for commodity Exchange)** Any new hardware and software addition/change hosted in COLO (including firmware changes) shall be thoroughly tested during mock or simulation market.
17(t)	Traffic Monitoring: (Applicable to COLO Members) **(Not applicable for commodity Exchange)** The member shall also monitor the traffic originating from Its own IT infrastructure hosted in COLO towards Exchange and put adequate controls to prevent any spurious/unwanted. traffic coming to Exchange.
17 (u)	LAMA System auditor shall verify whether the specified member has integrated all the critical systems in LAMA. Whether data from all the critical systems is being published in the LAMA server in accordance with MCX/TECH/726/2022, dated December 16, 2022.
18	**AI-ML**
18(a)	Are adequate safeguards in place to prevent abnormal behaviour of the AI or ML application / System.
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.
18(c)	Whether AI / ML systems comply for all above System Audit Checklist points. In case of any observation, please report.
19	**Undertaking/Application for CTCL/IBT/STWT/DMA/SOR**
19(a)	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)
20	**Pre Trade Risk Control**
20(a)	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.
21	**Asset Management**
21(a)	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? Whether the IT asset inventory contains the information regarding the hostname, IP Address, Asset Owner, Operating System details, Criticality of asset, Asset Tagging, end-of-life / end-of-support, last patched date, etc.

22	**Phishing & Malware Protection For IBT / STWT**
22(a)	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?
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:**
23(a)	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
24	**Remote Access Controls**
24(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?
24(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?
24(c)	Does the organization's 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 devices are not getting used for any purpose other than the use of remote access to data centre resources?
24(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?
24(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.
24(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?.

24(g)	Does the organization have appropriate risk mitigation mechanisms whenever remote access of data center resources is permitted for service providers?.
24(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?.
24(i)	Does the organizations backup, restore and archival functions work seamlessly, particularly if the users have remote access to internal systems.?
24(j)	Does the organization apply only necessary and applicable patches to the existing hardware and software?
24(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?
24(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
25	**SEBI and Exchange Compliances**
25(a)	Auditor to list all applicable Circulars, Notices, Guidelines, and advisories published by SEBI and Exchanges and mention
25(b)	1- Adherence to all such Circulars, Notices, Guidelines, and advisories published
25(c)	2- Reporting adherences based on prescribed periodicity in point 1 above

Note -: Some of the CTCL facilities like SOR and co-location may not be applicable to Commodity Derivative Exchanges auditor is required to refer related circular for the same. Specific TOR points pertaining to other than Commodity Derivative Segment to be marked as not applicable (NA).