**MCX Stock Exchange Limited**
**CTCL Department**

Circular No.: MCX-SX/CTCL/1477/2013 September 30, 2013

## Testing of software used in or related to Trading and Risk Management

In terms of the provisions of Rules, Bye-Laws and Regulations of the MCX Stock Exchange Limited ('Exchange'), Members of the Exchange are notified as under:

1. The Exchange vide its Circular No. MCX-SX/CTCL/925/2012 dated December 31, 2012 has laid down guidelines/directions to members on Computer to Computer Link (CTCL), Internet Based Trading (IBT), Algorithmic Trading (Algo), Direct Market Access (DMA), Securities Trading using Wireless Technology, Smart Order Routing (SOR), In-House CTCL software development by member and ISV empanelment.

2. In view of SEBI vide Circular No. CIR/MRD/DP/24/2013 dated August 19, 2013 regarding '**Testing of software used in or related to Trading and Risk Management**', CTCL/IBT/DMA/Wireless Trading/Algo/SOR facility (hereinafter referred as 'CTCL Facility') approval process of the Exchange has been modified with immediate effect and is as specified hereinafter. The new approval process will be applicable for member applications for empanelled ISVs software as well as In-house development.

3. **Approval to Member for 'CTCL Facility'**

3.1 The member will be required to give an undertaking to Exchange as per format provided in **Annexure I** along with the applicable documentation for respective 'CTCL Facility' as per Circular No. MCX-SX/CTCL/925/2012 dated December 31, 2012.

3.2 The member will have to test the software on the test environment provided by the Exchange. For this purpose a User Id on the test environment should be requested from the Exchange via email. The member should ensure that the software meets the minimum requirements outlined in **Annexure II.**

3.3 The testing of software shall also include successful participation by member in atleast one Mock Trading session conducted by Exchange. Further, it will be mandatory for members to participate in periodic Mock Trading sessions conducted by Exchange using all User Ids approved for Algo trading, irrespective of the algorithm having undergone change or not. In case the member fails to participate in such mock trading sessions, the Exchange shall call for reasons for non-participation and if the reason is found to be unsatisfactory, the Exchange shall suspend the proprietary trading rights of the member for a minimum period of one trading day.

3.4 The proposed software and system shall be duly certified by a system auditor who possess atleast one of the following certifications:

(a) CISA (Certified Information System Auditors) from ISACA;

(b) DISA (Post Qualification Certification in Information Systems Audit) from Institute of Chartered Accountants of India (ICAI);

(c) CISM (Certified Information Securities Manager) from ISACA;

(d) CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium, commonly known as (ISC).

The system audit charges shall be negotiated and paid directly by the member to the system auditor.

3.5 Members are required to submit the original copy of the report of the system audit conducted of their software and system to the Exchange along with the documents as per checklist mentioned in Circular No. MCX-SX/CTCL/925/2012 for the respective facility. The format of system audit report is enclosed as **Annexure III.** Members should ensure that the audit report submitted by them is strictly in accordance with the format specified. Any deviation in the format of the report would lead to rejection of submission.

3.6 The system audit report should be on the letter head of the system auditor. It may be noted that all the pages of the System Audit Report should be duly stamped and signed by the system auditor. The system audit report must contain the Name and registration number of system auditor along with their stamp, place and date at the end of report. The system auditor should categorically certify in the report about absence of conflict of interest as given in System Audit Report format.

3.7 The Exchange may require the demonstration of the software before granting an approval. Member shall arrange to provide demonstration of the software at Exchange premises, after taking a prior appointment with CTCL team. After successful demonstration of the software and on being satisfied with the documents submitted by the member, Exchange may grant permission to Member for the usage of 'CTCL Facility' or any part thereof.

3.8 The approval procedure will be applicable for first time approval to member and for Vendor change for their respective CTCL facility. Members already approved by the Exchange for respective CTCL facility will not be required to submit system audit report while applying for additional User Id for using same software.

3.9 However members may note that every Algo User Id of the member shall compulsorily participate in each mock trading session organised by the Exchange on an ongoing basis & details of such participation have to be covered in the periodic system audit reports.

4. **Modifications in Approved Software**

4.1 Member shall apply to Exchange for approval of any modifications/changes done in approved software and/or system and shall follow the procedure mentioned in **Paragraph 3** except that fresh Undertaking need not be submitted. Member shall deploy the modified software in Live Enviornmentonly after receiving Exchange approval for the same, after complying with all requirements of the Exchange as contatined herein.

5. **Penalty for the Malfunctioning of software**

5.1 Members may note that in terms of the aforesaid SEBI circular, the Exchange may take deterrent action in cases of malfunctioning of software.

6. **Applicability**

6.1.1 This Circular shall be effective immediately for members opting for the CTCL facility for the first time.

6.1.2 Members who are currently availing the CTCL faility shall submit an Undertaking in the format given in **Annexure I** latest by October 31, 2013 and shall ensure compliance.

For any clarifications kindly contact Customer Service on 022 - 67319010 / 66494030 or send an email to customerservice@mcx-sx.com.

**For and on behalf of**
**MCX Stock Exchange Limited**

**Mukesh Desai**
**Senior Manager**

Encl: As Above

**Annexure I**

## UNDERTAKING TO BE GIVEN BY TRADING MEMBER/ STOCK BROKER

I/We _____, an individual /a firm registered under the Indian Partnership Act, 1932 / a Company / body corporate incorporated under the Companies Act of 1956 and residing at / having our registered office at _____ give this UNDERTAKING on this _____ day of _____ at _____ IN FAVOUR of MCX Stock Exchange Ltd., a company incorporated under the Companies Act,of 1956, having registered office at Exchange Square, CTS No.255, Suren Road, Chakala, Andheri (East), Mumbai – 400 093 (hereinafter called 'Exchange').

**WHEREAS**

a) The Exchange has provided the trading software to enable its Members to trade on its trading platform.

b) The Exchange vide its Circular No. MCX-SX/CTCL/925/2012 dated December 31, 2012 had provided guidelines/directions on Computer to Computer Link (CTCL)/Internet Based Trading (IBT)/Algorithmic Trading (Algo)/Direct Market Access (DMA)/Securities Trading using Wireless Technology/Smart Order Routing (SOR) (hereinafter referred as 'CTCL Facility'), In-House CTCL software development by member and ISV empanelment.

c) SEBI vide their circular no: CIR/MRD/DP/24/2013 dated: August 19,2013 issued detailed guidelines on testing of software used in or related to trading and risk management to be adhered by the Stock Exchanges, Stock Brokers/ Trading Members and their vendors.

d) The Exchange had circulated the said SEBI circular for benefits of its members vide circular no. MCX-SX/CTCL/1395/2013 dated. August 21, 2013.

e) The undersigned member is already using or intending to use various software for trading and risk management as mentioned and hereby agrees to undertake and the abide by the following.

**NOW THEREFORE IN CONSIDERATION OF THE EXCHANGE** having agreed to consider my application to avail the CTCL Facility, I / We hereby IRREVOCABLY AND UNCONDITIONALLY UNDERTAKE and agree to abide by and be bound by the following terms and conditions:

1. I / We undertake that M/s _____ (Name of Trading Member) will take all necessary steps to ensure that every new software and any change thereupon to the trading and/or risk management functionalities of the software will be tested as per the framework prescribed by SEBI / Exchange before deployment of such new / modified software in securities market.

2. I / We undertake that M/s _____ (Name of Trading Member) will ensure that approval of the Exchange is sought for all new / modified software and will comply with various requirements specified by SEBI or the Exchange from time to time with regard to usage, testing and audit of the software.

3. I / We undertake that the absolute liability arising from failure to comply with the above provisions shall lie entirely with M/s _____ (Name of Trading Member).

4. I / we shall execute, sign and subscribe to such other documents, papers, agreements, covenants, bonds, and/or undertakings as may be prescribed or required by Exchange/SEBI from time to time.

5. I/We also agree and understand that in the event of my/our non-compliance with any of the provisions as mentioned above, Exchange shall take such action against us as it may deem fit in this regard including suspension, penalties, fines, etc.

6. I/ We shall indemnify and keep indemnified the Exchange, their directors, managers, officers, employees and agents harmless against every and all claims, demands, actions, proceedings, damages, liabilities, losses, costs and expenses suffered or incurred by them, which arises out of my/our usage of CTCL Facility.

7. I/We agree that this undertaking shall be governed by the laws of India and Courts at Mumbai shall have exclusive jurisdiction in all such matters arising out of this undertaking.

8. I/we hereby agree to abide by the Bye-laws, Rules, Regulations, Circulars and/or any other amendments issued by the Exchange/ SEBI from time to time.

IN WITNESS WHEREOF this Undertaking is executed by the undersigned on the day, month, year and the place first mentioned above.

SIGNED, SEALED AND DELIVERED BY

_____

For and on behalf of _____

_____

_____

Before me

Witness 1:

Witness 2:

# GUIDELINES FOR SUBMITTING UNDERTAKING

1. The Undertaking is to be executed on a non-judicial stamp paper/s or on paper franked from Stamp Office / authorised banks, for a value of ₹ 300/-

2. Further the Undertaking (including all annexures / schedules) has to be notarised before a Notary Public.

3. Please use the format of respective undertaking as it is. **PLEASE DO NOT RETYPE THE UNDERTAKING**.

4. All the pages of this Undertaking (including all annexures / schedules) have to be signed in full. The persons signing should also sign in full at all places in the Undertaking where anything has been hand-written / any corrections have been made.

   If the Trading Member is an individual, then the Undertaking has to be signed by the individual Trading Member himself. If the Trading Member is a firm, then ALL the partners are required to sign this Undertaking. If the Trading Member is a company, then the Undertaking has to be signed by the Managing Director or any Director of the company named as an authorised signatory of the company.

5. If the Trading Member is a company, the Undertaking has to be accompanied with a certified copy of the resolution of the Board of Directors of the company authorising the person(s) executing the undertaking to do so. The Common Seal of the company has to be affixed by the company on this Undertaking in the presence of such persons as authorised by the Articles of Association of the company. The Board Resolution should clearly state that the affixation of common seal shall be made in the presence of such persons as authorised by the Articles of Association of the company and should also clearly state the names of such persons. The above persons should sign the undertaking as a token of their presence when the common seal is affixed.

6. Please type the following on the non-judicial stamp paper as the first page and sign.

   The non-judicial stamp paper of Rs._____ forms part and parcel of this Undertaking executed by me/us Mr. /Mrs. /M/s. _____ having my/our residence/office at _____ on this the _____day of _____ 20___at _____IN FAVOUR of MCX Stock Exchange Limited.

Signature**

(**to be signed by the person(s) signing the Undertaking)

**Annexure II**

## Reference Points While Developing/Testing 'CTCL Facility' Software

- **Order Management**
  - Order entry- attributes
  - Order confirmation
  - Order status
  - Order modification
  - Order cancellation
  - Pending orders
  - Order history / reports

- **Trade management**
  - Trade confirmation
  - Trade Reports
  - Trade modification

- **Risk Management**
  - Exposure limit
  - Margin limit
  - Order Quantity Limits
  - Order Value Limits
  - Daily Price Range Checks
  - Cumulative limit on value of unexecuted orders

- **Client information**
  - Client code structure
  - Display of client position

- **Security & Compliance related**
  - Password protection
  - Lock-in mechanism for inactive users
  - Security of login session
  - Display of Trading member code and user id
  - Mandatory collection of margins
  - Display of Exchange User Id and TM name on trader workstation

- **Internet Trading**
  - Member name and SEBI registration no. on website
  - Display of Investor protection rule, Arbitration rule and rules effecting member - client relationship
  - Display of Risk disclosure documents
  - Trade confirmation through email and/or on the mobile phone
  - Default client code while order entry

**Annexure III**

**System Audit Report - Format**
(On the letterhead of system auditor)

Date:

Name of Trading Member:
Member Id:

1. **CTCL Audit Checklist (Part I)**
2. **IBT Audit Checklist (Part I + Part II)**
3. **Wireless Trading Audit Checklist (Part I + Part II + Part III)**
4. **Algo Audit Checklist (Part I + Part IV)**
5. **DMA Audit Checklist (Part I + Part V)**
6. **SOR Audit Checklist (Part I + Part VI)**

**PART I**

<table>
<tr><th>Sr. No.</th><th>Area of Audit</th><th>Results & Observations</th><th>Auditor's Remark</th></tr>
<tr><td>A.</td><td>System Features & Functionality</td><td>Results</td><td>Opinions</td></tr>
<tr><td>1.</td><td>Software Details<br><br>
<table>
<tr><th>Particulars</th><th>Name</th><th>Version No</th></tr>
<tr><td>Application software</td><td></td><td></td></tr>
<tr><td>Software developed by</td><td></td><td>----</td></tr>
<tr><td>Gateway/Adapter</td><td></td><td></td></tr>
<tr><td>Risk Administration / Manager</td><td></td><td></td></tr>
<tr><td>Front End / Order Placement / Algo Strategy</td><td></td><td></td></tr>
<tr><td>Database details</td><td></td><td>----</td></tr>
</table></td><td></td><td></td></tr>
<tr><td>2.</td><td>The installed system features are as prescribed by MCX-SX.<br><br>The Member ensures that software version number is used to identify the system being approved by the Exchange.<br><br>Price Broadcast<br>The system has a feature for receipt of price broadcast data<br><br>Order Processing :<br>The system has a feature:<br>a) Which allows order entry and confirmation of orders<br>b) Which allows for modification or cancellation of orders placed<br><br>Trade Confirmation:<br>The system has a feature which enables confirmation of trades.</td><td></td><td></td></tr>
<tr><td>3.</td><td>The installed system provides a system based control facility over the order input process<br><br>Order Entry<br>The system has order placement controls that allow only orders</td><td></td><td></td></tr>
</table>

| | | | |
|---|---|---|---|
| | matching the system parameters to be placed.<br><br>Order Modification<br>The system allows for modification of orders placed.<br><br>Order Cancellation<br>The system allows for cancellation of orders placed Order Outstanding Check<br>The system has a feature for checking the outstanding orders i.e. the orders that have not yet traded or partially traded. | | |
| 4. | **The installed system provides a system based control facility over the trade confirmation process**<br><br>Trade Confirmation and Reporting Feature<br><br>Should allow confirmation and reporting of the orders that have resulted in trade | | |
| 5. | **The installed system provides a system based control facility over the order input process**<br><br>Order Matching<br>Does the System pass all the Orders to the trading platform of the Exchange for execution and not allow any crossing of orders that are routed through it? | | |
| 6. | The System generates appropriate audit logs and trails so as to facilitate tracking of events such as orders and trades with timestamp. | | |
| 7. | **The installed system allows for placing of orders only for authorized clients**<br><br>Client ID Verification<br>Only duly authorized client's orders are allowed to be placed.<br><br>Proprietary order entry mechanism<br>Order entry for Pro types of orders is executed through specific User Ids.<br><br>The system should not in any manner suggest to the user by default the name of Exchange, Scrip and Segment etc. It is the user who should have the option to select the same. | | |
| 8. | **The installed system has a User Management system as per the requirements of MCX-SX.**<br><br>Approved Users:<br>Only users approved by MCX-SX are allowed to access the system and documentation regarding the same is maintained in the form of<br>a) User Approval Application<br>b) Copy of User Qualifications<br><br>User Creation:<br>New User IDs are created as per the CTCL guidelines.<br><br>User ID: | | |

| | | | |
|---|---|---|---|
| | All users are uniquely identified through issue of unique CTCL ids.<br><br>User Disablement:<br>Users not compliant with the Exchange Requirements are disabled and event logs maintained<br><br>User Deletion:<br>Users are deleted as per the MCX-SX guidelines<br><br>Reissue of User Ids:<br>User Ids are reissued as per the MCX-SX guidelines.<br><br>Locked User Accounts:<br>Users whose accounts are locked are unlocked only after documented unlocking requests are made. | | |
| 9. | Whether all successful and failed login attempts are logged with details like IP address, MAC address and other data to enable traceability | | |
| **B.** | **Risk Management System** | Results | Opinions |
| 10. | **The installed system is capable of assessing the risk of the client as soon as the order comes in and informs the client of acceptance/rejection of the order within a reasonable period.**<br>Should allow for risk management of the orders placed and online risk monitoring of the orders being placed.<br><br>Order Parameters<br>There is online risk assessment of all orders placed through the system. | | |
| 11. | Whether the system carries out appropriate validations of the following risk parameters including Credit checks before the orders are released to the Exchange:<br>a) Exposure limit<br>b) Margin limit<br>c) Order Quantity Limits<br>d) Order Value Limits<br>e) Daily Price Range Checks<br>f) Cumulative limit on value of unexecuted orders | | |
| 12. | **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.**<br><br>The installed systems has a provision for On-line surveillance and risk management as per the requirements of MCX-SX and includes<br>Number of Users Logged In / hooked on to the network incl. privileges of each<br><br>The installed systems has a provision for off line monitoring and risk management as per the requirements of MCX-SX and includes reports / logs on<br>a) Number of Authorized Users | | |

| | | | |
|---|---|---|---|
| | b) Activity logs<br>c) Systems logs<br>d) Number of active clients | | |
| 13. | **The installed system provides a system based control facility on the trading limits of the clients and exposures taken by the clients including set pre-defined limits on the exposure and turnover of each client.**<br><br>Only orders that are within the parameters specified by the risk management systems are allowed to be placed. | | |
| 14. | System-based control on the pre-defined trading limits set by the Member. | | |
| 15. | **The installed system provides for reconfirmation of orders which are larger than that as specified by the member's risk management system.**<br><br>Whether system has a manual override facility for allowing orders that do not fit the system based risk control parameters? | | |
| 16. | Facility to prompt the user when he puts in orders that are over and above the normal limits set by the Member. | | |
| **C.** | **Session Security** | Results | Opinions |
| 17. | Whether system has secure end-to-end encryption for all data transmission between the client and the member system through a Secure Standardized Protocol.<br>A procedure of mutual authentication between the client and the member server is implemented? | | |
| 18. | **The installed system provides for session security for all sessions established with the server by the front end application.**<br>a) The system uses session identification and authentication measures to restrict sessions to authorized user only.<br>b) The system uses session security measures like encryption to ensure confidentiality of sessions initiated. | | |
| 19. | **The installed system has provision for security, reliability and confidentiality of data through use of encryption technology, SSL or similar session confidentiality protection mechanisms**<br><br>a) The system uses SSL or similar session confidentiality protection mechanisms<br>b) The system uses a secure storage mechanism for storing of usernames and passwords<br>c) The system adequately protects the confidentiality of the user's trade data. | | |
| **D.** | **Password Security** | Results | Opinions |
| 20. | Does the organization's policy and procedure document have a password policy? | | |
| 21. | **The installed system Authentication mechanism is as per the guidelines of the MCX-SX**<br><br>a) The installed system's uses passwords for authentication.<br>b) The system requests for identification and new password before login into the system.<br>c) The Password is masked at the time of entry. | | |

| | | | |
|---|---|---|---|
| 22. | System authenticates user with a User Name and password as first level of security. | | |
| 23. | System mandates changing of password when the user logs in for the first time? | | |
| 24. | Automatic disablement of the user on entering erroneous password on five consecutive occasions. | | |
| 25. | The system provides for automatic expiry of passwords at the end of a reasonable duration (maximum 6 months) and re-initialisation of access on entering fresh passwords. | | |
| 26. | Prior intimation is given to the user before such expiry? | | |
| 27. | System controls to ensure that the password is alphanumeric (preferably with one special character), instead of just being alphabets or just numerical. | | |
| 28. | System controls to ensure that the changed password cannot be the same as of the last 6 passwords. | | |
| 29. | System controls to ensure that the Login id of the user and password should not be the same. | | |
| 30. | System controls to ensure that the Password should be of minimum six characters and not more than twelve characters. | | |
| 31. | User is deactivated if the same is not used for a continuous period of 12 (Twelve) months from date of last use of the account. | | |
| 32. | System allows user to change their passwords at their discretion and frequency. | | |
| 33. | 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. | | |
| **E.** | **Infrastructure & Capacity Management** | Results | Opinions |
| 34. | System has built-in high system availability to address any single point failure. | | |
| 35. | Service has adequate bandwidth and multiple links to ensure reliability and redundancy. | | |
| 36. | Are the resources monitored, tuned and calculations made for future capacity requirements to ensure the required performance. | | |
| 37. | Adequate un-interrupted power supply for smooth operation of the System is available at the Site? | | |
| 38. | Whether backup network link is available in case of failure of the primary link to the MCX-SX? | | |
| 39. | **Firewall**<br><br>Whether suitable firewalls are implemented? | | |
| 40. | **Anti virus**<br><br>Is a malicious code protection system implemented? If Yes, then<br><br>Are the definition files up-to-date?<br><br>Any instances of infection?<br><br>Last date of virus check of entire system. | | |
| 41. | **Additional Access Control Security**<br>**The installed system provides a dual factor authentication** | | |

| | | | |
|---|---|---|---|
| | **system for access to the various components.**<br><br>Extra Authentication Security<br>a) The systems uses additional authentication measures like smart cards, biometric authentication or tokens etc.<br>b) The system has a second level of password control for critical features. | | |
| **F.** | **Backup & Recovery Procedures** | Results | Opinions |
| 42. | Does the organization's documented policy include a backup policy and procedures? | | |
| 43. | The back-up and restore systems implemented by the member is adequate to deliver sustained performance and high availability.<br>Whether the member system has on-site as well as remote site back-up capabilities? | | |
| 44. | **The Installed systems backup capability is adequate as per the requirements of the MCX-SX for overcoming loss of product integrity.**<br><br>Are backups of the following system generated files maintained as per the MCX-SX guidelines?<br>a) At the server/gateway level<br>b) Database<br>c) Audit Trails Reports<br><br>At the user level<br>a) Market Watch<br>b) Logs<br>c) History<br>d) Reports<br>e) Audit Trails<br><br>Are backup procedures documented and backup logs maintained?<br><br>Are the backup logs maintained and are the backups been verified and tested?<br><br>Are the backup media stored safely in line with the risk involved?<br><br>Are there any recovery procedures and have the same been tested? | | |
| **G.** | **Business Continuity & Disaster Recovery Procedures** | Results | Opinions |
| 45. | **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**<br><br>Is there any documentation on Business Continuity / Disaster Recovery / Incident Response?<br><br>Does a BCP / DRP plan exist?<br><br>If a BCP/DRP plan exists, has it been tested? | | |

| | | | |
|---|---|---|---|
| | Are there any documented incident response procedures?<br><br>Are there any documented risk assessments?<br><br>Does the installation have a Call List for emergencies maintained? | | |
| 46. | **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**<br><br>Is the backup network link adequate in case of failure of the primary link to the MCX-SX?<br><br>Is the backup network link adequate in case of failure of the primary link connecting the users?<br><br>Is there an alternate communications path between customers and the firm?<br><br>Is there an alternate communications path between the firm and its employees?<br><br>Is there an alternate communications path with critical business constituents, banks and regulators? | | |
| 47. | **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**<br><br>Are there suitable backups for failure of any of the critical system components like<br>a) Gateway / Database Server<br>b) Router<br>c) Network Switch<br><br>Infrastructure breakdown backup<br>Are there suitable arrangements made for the breakdown in any infrastructure components like<br>a) Power Supply<br>b) Water<br>c) Air Conditioning<br><br>Primary Site Unavailability<br>Have any provision for alternate physical location of employees been made in case of non availability of the primary site<br><br>Disaster Recovery<br>Are there suitable provisions for Books and records backup and recovery (hard copy and electronic).<br><br>Have all mission-critical systems been identified and provision for backup for such systems been made? | | |

| | | | |
|---|---|---|---|
| 48. | In case of failure of Internet, the alternate channel of communication has adequate capabilities for client identification and authentication. | | |
| **H.** | **Operational Integrity** | Results | Opinions |
| 49. | Does the organization's policy and procedure document have an access control policy for users of the service? | | |
| 50. | **The installed system provides a system based access control over the server as well as the risk management and front end dealing applications while providing for security**<br><br>Access controls<br>a) The system allows access to only authorized users<br>b) The system has a password mechanism which restricts access to authenticate users. | | |
| 51. | **Physical Security**<br><br>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? | | |
| 52. | **To ensure information security for the Organisation in general and the installed system in particular policy and procedures as per the MCX-SX requirements must be established, implemented and maintained.**<br><br>Does the organization's documented policy and procedures include the following policies and if so are they in line with the MCX-SX requirements?<br>a) Information Security Policy<br>b) Password Policy<br>c) User Management and Access Control Policy<br>d) Network Security Policy<br>e) Application Software Policy<br>f) Change Management Policy<br>g) Backup Policy<br>h) BCP and Response Management Policy<br>i) Audit Trail Policy<br><br>Does the organization follow any other policy or procedures or documented practices that are relevant? | | |
| 53. | The Member ensures that the persons supporting the service possess requisite skills for technical support, System administration and other related functions pertaining to the System. | | |
| 54. | **Are documented practices available for various system processes**<br><br>Day Begin<br><br>Day End<br><br>Other system processes<br>a) Audit Trails<br>b) Access Logs<br>c) Transaction Logs | | |

| | | | |
|---|---|---|---|
| | d) Backup Logs<br>e) Alert Logs<br>f) Activity Logs<br>g) Retention Period<br>h) Data Maintenance | | |
| 55. | **In case of failure, is there an escalation procedure implemented?**<br><br>Day Begin<br><br>Day End<br><br>Other system processes<br><br>Details of the various response procedures including for<br>a) Access Control failure<br>b) Day Begin failure<br>c) Day End failure<br>d) Other system Processes failure | | |
| 56. | **To ensure system integrity and stability all changes to the installed system are planned, evaluated for risk, tested, approved and documented.**<br><br>Planned Changes<br>a) Are changes to the installed system made in a planned manner?<br>b) Are they made by duly authorized personnel?<br>c) Risk Evaluation Process<br>d) Is the risk involved in the implementation of the changes duly factored in?<br><br>Change Approval<br>Is the implemented change duly approved and process documented?<br><br>Pre-implementation process<br>Is the change request process documented?<br><br>Change implementation process<br>Is the change implementation process supervised to ensure system integrity and continuity<br><br>Post implementation process<br>Is user acceptance of the change documented?<br><br>Unplanned Changes<br>In case of unplanned changes, are the same duly authorized and the manner of change documented later?<br><br>In case of members self developed system<br>SDLC documentation and procedures if the installed system is developed In-House. | | |
| **I.** | **Approvals, Undertaking, Policies and Other Area** | Results | Opinions |

| | | | |
|---|---|---|---|
| 57. | **Insurance** The insurance policy of the Member covers the additional risk of usage of system and probable losses in case of software malfunction. | | |
| 58. | **Settlement of Trades**<br>**The installed system provides a system based reports on contracts, margin requirements, payment and delivery obligations**<br><br>Margin Reports feature<br>Should allow for the reporting of client wise / user wise margin requirements as well as payment and delivery obligations. | | |
| 59. | **Database Security**<br><br>a) The installed system has sufficient controls over the access to and integrity of the database<br>b) The access to the database is allowed only to authorized users / applications.<br>c) The database is hosted on a secure platform.<br>d) The database stores the user names / passwords securely. | | |
| 60. | Whether system has adequate safety features to ensure it is not susceptible to internal / external attacks? | | |
| 61. | Is there any other area/aspect which in the auditor's opinion is not complied with and which is significant and material in relation to the size and the nature of the operations? | | |
| 62. | Whether the required details of all the 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?<br><br>If no, please give details | | |
| 63. | Whether all the 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?<br><br>If no, please give details | | |
| **J.** | **Software Testing Verification** | **Results** | **Opinions** |
| 64. | **Verification of software testing done by Member in Exchange provided Test environment**<br><br>Whether member has tested the Software in Exchange provided Test Environment<br>Details<br>a) No. of days software has been tested by member in Exchange provided Test environment<br>b) Member Id & User Id used by member for testing in the Exchange provided Test environment<br><br>Whether any abnormalities observed in the verification of Logs, | | |

| | | | |
|---|---|---|---|
| | Reports, Audit Trail and Database of the tests performed by member in Exchange provided Test environment | | |
| 65. | **Verification of participation by Member in Periodic Mock Trading session conducted by Exchange**<br><br>Whether member has participated in Mock Trading sessions conducted by Exchange (Minimum 1 before approval)<br><br>Details<br><br>**Sr #** \| **Mock Trading Date** \| **Segment** \| **User ID** \| **CTCL/IBT/Wireless Trading/DMA/ALGO/SOR**<br>\| \| \| \| \|<br><br>Whether any abnormalities observed in the verification of Logs, Reports, Audit Trail and Database of the tests performed by member while participating in Periodic Mock Trading session conducted by Exchange | | |

**PART II**

| Sr. No. | Area of Audit | Results & Observations | Auditor's Remark |
|---|---|---|---|
| | **System Features & Functionality** | Results | Opinions |
| 1. | View Order status i.e. the orders that have not yet traded or partially traded or cancelled<br><br>Order Confirmation | | |
| 2. | Acceptance / rejection of an order / trade is communicated to the IBT client. | | |
| 3. | **Order Capture / Status** should capture the following information:<br>Order Id generated by the Exchange<br><br>IBT Client ID and type of IBT Client<br><br>Date and Time of order placement<br><br>Scrip name / code / symbol<br><br>Action (Buy/Sell)<br><br>Quantity (ensure market lot)<br><br>Order type (Regular Lot / Stop Loss or such orders as allowed by Exchange)<br><br>Order validity (type as permitted by exchange such as Day, EOS, IOC)e | | |

| | | | |
|---|---|---|---|
| | Price (Ensure DPR -price band / circuit limit and minimum tick size as allowed by Exchange)<br><br>Execution status<br><br>System captures the IP address (from where the orders are originating) for all IBT orders | | |
| 4. | Is the trade confirmation sent to the client via e-mail? | | |
| 5. | Can the IBT client choose the interval of receiving the e-mail? | | |
| 6. | Whether a unique identification number as prescribed by Exchange (i.e. 111111111111 in CTCL Unique number) is sent with each IBT Order? | | |
| 7. | Two-factor authentication for login session has been implemented for all IBT orders emanating using Internet Protocol? | | |
| | **Risk Management System** | Results | Opinions |
| 8. | Whether System-based control is implemented by the Member for the Margin, Order Quantity and Value? | | |
| 9. | IBT Member shall ensure that logic / priorities used by the Exchange are followed by the System for treating IBT Client Orders. | | |
| | **Session Security** | Results | Opinions |
| 10. | In case of no activity by the IBT client, the system provides for automatic trading session logout. | | |
| | **Password Security** | Results | Opinions |
| 11. | Does the organization's policy and procedure document have an access control policy for users of the service? | | |
| 12. | Whether all successful and failed login attempts are logged with details like IP address, MAC address and other data to enable traceability | | |
| | **Operational Integrity** | **Results** | **Opinions** |
| 13. | The IBT member ensures that a specific email id to receive mails from IBT Clients is communicated to all clients. | | |
| 14. | Member has documented and implemented a procedure to escalate the issue if the email is not responded within one working day. | | |
| | **Approvals, Undertaking, Policies and Other Area** | **Results** | **Opinions** |
| 15. | Display of Investor protection rule, Arbitration rule and rules effecting member - client relationship on approved IBT member's website. | | |
| 16. | The web site of IBT approved member provides and displays prominently hyper link to the web site/page on the web site of the MCX-SX displaying rules/Business Rules/circulars. | | |

**Part III**

| Sr. No. | Area of Audit | Results & Observations | Auditor's Remark |
|---|---|---|---|
| | **System Features & Functionality** | Results | Opinions |
| 1. | The installed Wireless Trading system provides a system based control facility over the trade confirmation process<br><br>Trade Confirmation and Reporting Feature | | |

| | | | |
|---|---|---|---|
| | Should allow confirmation and reporting of the orders that have resulted in trade<br>As it may not be possible to give detailed information about the order status on a hand held device e.g. mobile phones, it should be ensured that minimum information may be given with addresses of the Internet web site / web page where detailed information would be available. | | |
| 2. | The installed Wireless Trading system provides a system based control facility over the order input process<br><br>Order Identification Methodology<br>A unique identification number for each Wireless Trading<br><br>System captures the IP address (from where the orders are originating) for all Wireless Trading orders? | | |
| 3 | Whether a unique identification number as prescribed by Exchange (i.e. 333333333333 in CTCL Unique number) is sent with each Order originating from a wireless device? | | |
| 4. | Whether audit trails are provided to the user on the wireless device? | | |
| | **Session Security** | Results | Opinions |
| 5. | In case of no activity by the Wireless Trading client, the system provides for automatic trading session logout. | | |
| 6. | In case of Wireless Trading whether provision has been made to lock the trading application in case of loss of the hand held device? | | |
| 7. | It must be ensured that the session login details should not be stored on the devices used for Wireless Trading. | | |

**Part IV**

| Sr. No. | Area of Audit | Results & Observations | Auditor's Remark |
|---|---|---|---|
| | **Operational Specifications** | Results | Opinions |
| 1. | Whether all algo orders are necessarily routed through member's servers located in India? | | |
| | **Risk Management System** | Results | Opinions |
| 2. | Whether the Algo software provides for routing of orders through electronic / automated risk management systems of the member to carry out appropriate validations of all risk parameters before released to the Exchange trading system including individual Order level such as:<br>a) Price check – Algo orders shall not be released in breach of the price bands defined by the Exchange for the security / contract.<br><br>b) Quantity check – Algo orders shall not be released in breach of the quantity limit as defined by the Exchange for the | | |

| | | | |
|---|---|---|---|
| | security / contract.<br><br>c) Order Value check - Algo orders shall not be released in breach of the 'value per order' as defined by the Exchange.<br><br>d) Cumulative Open Order Value check – The individual client level cumulative open order value check as may be prescribed by the member for the clients and Algo orders shall not be released in breach of the same. Cumulative Open Order Value for a client is the total value of its unexecuted orders released from the member's system.<br><br>e) Automated Execution check – An Algo shall account for all executed, unexecuted and unconfirmed orders, placed by it before releasing further order(s). Further, the Algo system shall have pre-defined parameters for an automatic stoppage in the event of Algo execution leading to a loop or a runaway situation.<br><br>f) Market Price Protection – Algo users shall not send MARKET order (i.e. order without any price) to Exchange. Algo users should send Market protection order instead of Market Order. The Market Protection order will be a LIMIT order with a price which will be computed automatically based on plus or minus 'x%' of LTP within the maximum range of DPR/dummy circuit filter.<br><br>g) Cumulative limit on value of unexecuted orders. | | |
| 3. | Whether member has real-time monitoring systems to identify algorithms that may not behave as expected? | | |
| | **System Features & Functionality** | Results | Opinions |
| 4. | Whether orders generated by Algo are identified as Algorithmic Trading orders while releasing to the Exchange.<br>For identification of Algo orders, members are required to ensure that the 13th digit of CTCL Terminal Information, which indicates whether the order is generated through Algo software or not, should be '1' if order is generated through Algo software. | | |
| | **Operational Integrity** | Results | Opinions |
| 5. | Whether Algo software has facility for generating and maintaining complete audit trail<br><br>Logs of all trading activities is available to facilitate audit trail.<br><br>Whether record of control parameters, orders, trades and data points emanating from trades executed through Algo are maintained by member.<br><br>Whether all logs generated are secured from unauthorised modifications? | | |
| 6. | Whether orders generated by Algo software are offered to the market for matching and system does not allow any crossing of orders with each other that are routed through it? | | |

| | | | |
|---|---|---|---|
| 7. | Whether system has sufficient security features including password protection for User Id, automatic expiry of password at the end of a reasonable duration and reinitialisation of Access on entering fresh password?<br><br>Whether registration and de-registration of users id are carried out as per the approved policy? | | |
| 8. | Whether member has procedures and arrangements to safeguard Algo from misuse or unauthorized access?<br>Whether adequate controls have been implemented for admission of personnel into the server rooms / place where algo servers are located and whether audit trails of all the entries / exits at the server room / location are maintained? | | |
| 9. | Any changes / upgrades done to the Algo software and system post approval by the Exchange. | | |
| 10. | Whether member has proper procedures, systems and technical capability to carry out trading through the use of Algo? | | |

**Part V**

| Sr. No. | Area of Audit | Results & Observations | Auditor's Remark |
|---|---|---|---|
| | **Operational Specifications** | Results | Opinions |
| 1. | Whether the Trading Member's server, routing the Direct Market Access (DMA) orders to the Exchange trading system is located in India? | | |
| 2. | Whether a unique identification number as prescribed by Exchange (i.e. 222222222222 in CTCL Unique number) is sent with each DMA Order? | | |
| 3. | Whether the DMA server application has the facility to enable & disable a DMA client? | | |
| 4. | Whether the DMA server application handles the order on first-cum-first basis across all DMA clients? | | |
| 5. | Whether the Trading Member's server application has an appropriate flag to identify separately DMA orders / trades? | | |
| 6. | Does the DMA System have a facility to maintain and retain all orders, trades, alert logs / activity logs with audit trail facility for at least 5 years? | | |
| 7. | Whether Position Limits specified for respective segment as specified by the Exchange / regulatory authorities:<br>a) Market-wide across all clients<br>b) Client-wise | | |
| 8. | Based on the Margin requirements as set out by the Exchange from time to time, the DMA application is able to limit the Net position of a DMA client that can be outstanding. | | |
| 9. | Whether appropriate limits for securities subject to FII limits as specified by the Exchange / Regulatory authorities can be set and DMA server application will notify the DMA client and / or control such orders before release to the Exchange | | |
| 10. | Whether provision is made in the DMA application for Trading | | |

| | | | |
|---|---|---|---|
| | member to set any other risk parameter? If yes, please provide details | | |
| 11 | Is there an adequate facility for issuing contract notes to the client within 24 hours of the trade execution? | | |
| | **Client Authorizations & Terms and Conditions** | **Results** | **Opinions** |
| 12. | Are the clients availing DMA facility authorized after fulfilling Terms and Conditions as per Exchange requirements? | | |
| 13. | Whether individual users at the client end are also authorized based on minimum criteria? | | |
| 14. | Are the Terms and Conditions as prescribed in Exchange Circular in place?<br>Whether the Exchange prescribed Terms and Conditions and formats as prescribed in Exchange Circular has been / will be adopted?<br>Or<br>The Terms and Conditions and formats will be modified? | | |
| 15. | Whether the DMA application is so designed that it allows execution of designated DMA client's orders only. DMA client should not have the facility to change it to any other persons/entity? | | |

**Part VI**

| Sr. No. | Area of Audit | Results & Observations | Auditor's Remark |
|---|---|---|---|
| | **Operational Specifications** | **Results** | **Opinions** |
| 1. | Whether the Trading Member's server, routing the SOR orders to the Exchange trading system is located in India? | | |
| 2. | The SOR system does not release orders to venues other than the recognized stock Exchange (Specify the list of recognized Stock Exchange(s) and the market segments to which SOR release orders) | | |
| 3. | Does the SOR application handle the order on first-cum-first basis across all the clients? | | |
| 4. | Whether Member is using similar logic/ priorities as used by Exchange to treat SOR client orders. | | |
| 5. | Whether SOR facility is provided to all class of investor? | | |
| 6. | In case the client has availed SOR facility and does not want to use the same for a particular order, whether the application provides the client with this facility. | | |
| 7. | Whether SOR facility is provided for all orders, without restricting to any specific type of order. The choice of order type shall be left to the client. | | |
| 8. | Whether orders generated by SOR facility are identified as SOR orders while releasing to the Exchange.<br>For identification of SOR orders, members are required to ensure that the 13th digit of Terminal Information, which indicates whether the order is generated through SOR software or not,<br>It should be '2' if order is generated through Smart Order without Algo Trading.<br>It should be '3' if order is generated through Smart Order with Algo | | |

| | | | |
|---|---|---|---|
| | Trading. | | |
| 9. | Order and Trade data should be readily available for query to the clients at least till the payout date of the transaction. | | |
| 10. | System ensures real time consolidation of price view based on priority of liquidity and prices prevailing in the exchanges. | | |
| 11. | The market prices are received directly from recognized stock Exchanges and are time stamped | | |
| 12. | The market prices of all the recognized stock exchanges to which the SOR facility routes orders are consolidated for applying the Best Execution Policy for routing orders | | |
| 13. | Whether the SOR application monitors best bids and offers and updates instantly as the market moves:<br>a) Does SOR system neutral to the participating exchanges and ensure best execution policy without induced time delay etc.<br>b) Does the SOR system adheres and includes necessary location ID or any such tagging specified by the Exchange from time to time.<br>c) Is there a proper standard operating procedure put in place for handling request / approval process for implementing SOR within the organization. | | |
| 14. | Does the SOR application have an appropriate flag to identify separately SOR orders and trades? | | |
| | **Risk Management** | Results | Opinions |
| 15. | The SOR application is so designed, configured and integrated with Order Routing server (ORS) so as to route the SOR orders only through electronic / automated risk management system where the trading member sets the risk profile of the SOR client. | | |
| 16. | Whether appropriate limits for securities subject to FII limits as specified by the Exchange / Regulatory authorities can be set and SOR server application will notify the SOR client and / or control such orders before release to the Exchange | | |

**Summary Sheet**

| Sr. No. | Area of Audit | Control / Processes | Compliance S / M / W | Report Reference |
|---|---|---|---|---|
| 1 | System Features & Functionality | Gateway & System Parameters | | |
| | | Application Features | | |
| | | Order Management | | |
| 2 | Risk Management System | Application Features | | |
| | | System Parameters | | |
| 3 | Session Security | Session Security Parameters | | |

| | | | | |
|---|---|---|---|---|
| | | Encryption Technologies | | |
| 4 | Password Security | Policies & Procedures | | |
| | | Password Implementation | | |
| 5 | Infrastructure & Capacity Management | Network & Redundant Connectivity | | |
| | | Scalability | | |
| | | Dependability | | |
| 6 | Backup & Recovery Procedures | Policies & Procedures | | |
| | | Backup & Archival process | | |
| 7 | Business Continuity & Disaster Recovery | Policies & Procedures | | |
| | | System Failure Backup | | |
| | | Disaster Recovery | | |
| 8 | Operational Integrity | Server Room / Network Room / Information Security | | |
| | | Qualified Personnel & Problem Escalation | | |
| | | Change Management | | |
| 9 | Vulnerability Assessment | Database | | |
| | | Operating System | | |
| 10 | Software Testing | Testing in Exchange provided Test environment | | |
| | | Testing & participation in Exchange conducted Mock Trading | | |
| 11 | Any Other area/aspect which in the auditors opinion is not complied with and which is significant and material in relation to the size and the nature of the operations | | | |

Overall rating for the Member's software and system: _____ (S / M / W)

Note: Process Area Controls Evaluation Criteria

| Control Evaluation Criteria | Description |
|---|---|
| Strong | The controls are defined as Strong if the following criteria are |

| | |
|---|---|
| | met<br><br>Implemented controls fully comply with the stated objectives and no material weaknesses are found. |
| Medium | The controls are defined as Medium if the following criteria are met<br><br>Implemented controls substantially comply with the stated objectives and no material weakness result in substantial risk exposure due to the non-compliance with the criteria<br>Compensatory controls exist which reduce the risk exposure to make it immaterial vis-à-vis the non-compliance with the criteria. |
| Weak | The controls are defined as Weak if the following criteria are met<br><br>Implemented controls materially fail to comply with the stated control objectives.<br>Compensating controls fail to reduce the risk so as to make it immaterial vis-à-vis the non-compliance with the compliance criteria. |

It is hereby confirmed and certified that system audit of the software and systems used by _____, a member of MCX Stock Exchange Limited ('Exchange') has been conducted by me and have been found to be in compliance with the requirements stipulated by SEBI and Exchange. The software and system have capacity to meet all requirements of the Exchange and SEBI as on date.

We certify that none of the current Directors / Partners / Promoters of the member are directly or indirectly related with any of the Directors / Promoters / Partners of _____(Name of Auditing Firm) and there is no conflict of interest with respect to the member being audited.

_____

Signature

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

Date:
Place:
Stamp/Seal: