Stock Broker System Audit Framework

Audit Process

1. System Audit of stock brokers should be conducted with the following periodicity
    a. Annual system audit is prescribed for stock brokers who satisfy any of the following criteria.
        i. Stock Brokers who use [**Computer-to-Computer Link (CTCL)** or **Intermediate Messaging Layer (IML)**][1] **/ Internet Based Trading (IBT)/ Direct Market Access (DMA)/ Securities Trading using Wireless Technology (STWT) / Smart Order Routing (SOR)** and have presence in more than 10 locations or number of terminals are more than 50.
        ii. Stock Brokers who are depository participants or are involved in offering any other financial services.

    b. Half yearly system audit has been prescribed for stock brokers who use Algorithmic Trading or provide their clients with the facility of Algorithmic Trading as per SEBI Circular CIR/MRD/16/2013 dated May 21, 2013**.**

    c. For all other stock brokers, system audit shall be conducted once in two years.

2. Such audit shall be conducted in accordance with the Norms, Terms of Reference (ToR) and Guidelines issued by SEBI and / or by stock exchanges. Separate ToRs are specified for the following categories of brokers:
    a. **Type I Broker**: Brokers who trade through exchange provided terminals such as NSE's NEAT, BSE's BOLT, MCX-SX's TWS, etc. (ToR attached as Annexure I);
    b. **Type II Broker**: Brokers who trade through API based trading terminals like [CTCL or IML] or IBT/DMA/STWT or SOR facility and who may also be TYPE I Brokers. (ToR attached as Annexure II)
    c. **Type III Broker**: Brokers who use Algorithmic Trading facility to trade and who may also be TYPE II Brokers. (ToR attached as Annexure III)

3. Stock brokers shall select auditors as per the selection norms provided in the guidelines and directions issued by stock exchanges and SEBI from time to time. The Auditor may perform a maximum of 3 successive audits of the stock broker.

4. The stock exchanges shall periodically review ToR of such system audit and, if required, shall suitably revise the ToR after taking into consideration developments that have taken place in the securities market since the last review of ToR, observations reported in the audit reports of the stock brokers and directions issued by SEBI from time to time in this regard.

5. The auditor in its report shall specify compliance / non-compliance status with regard to areas mentioned in ToR. Observations on minor / major deviations as well as qualitative comments for scope for improvement shall also be specified in the report. The auditor shall also take into consideration the observations / issues mentioned in the previous audit reports and cover open items in the report. The audit report submitted by the auditor should

[1] **or other similar trading facilities**

be forwarded to the stock exchange by the Stock Broker along with management comments, within 1 month of submission of report by the auditor.

6. Stock exchange shall ensure that the management of the stock broker provides their comment about the non-compliance / non-conformities (NCs) and observations mentioned in the report. For each NC, specific time-bound (within 3 months of submission of report by the exchange) corrective action must be taken and reported to the stock exchange. The auditor should indicate if a follow-on audit is required to review the status of NCs.

7. In order to ensure that the corrective actions are taken by the stock broker, follow-on audit, if any, shall be scheduled by the stock broker within 6 months of submission of the audit report by the system auditor.

8. The system auditors should follow the reporting standard as specified in Annexure –IV of this Framework for the executive summary of the System Audit report to highlight the major findings of the System Audit.

Auditor Selection Norms

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

2. It is recommended that resources employed shall have relevant industry recognized certifications e.g. D.I.S.A. (ICAI) Qualification , CISA (Certified Information System Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium, commonly known as (ISC).

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

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

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.

Annexure I

Terms of Reference (ToR) for Type I Broker

The system auditor shall at the minimum cover the following areas:

1. **System controls and capabilities**

    a. **Order Tracking** – The system auditor should verify system process and controls at exchange provided terminals 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.

    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.

    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 and at the servers of respective stock exchanges.

    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.

    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.

2. **Risk Management System (RMS)**

    a. **Online risk management capability –** The system auditor should check whether the system of online risk management (including upfront real-time risk management) is in place for all orders placed through exchange provided terminals.

    b. **Trading Limits –**Whether a system of pre-defined limits / checks such as Order Quantity and Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order Limit, Order Price limit, etc) are in place and only such orders which are within the parameters specified by the RMS are allowed to be pushed into exchange trading engines. The system auditor should check that no user or branch in the system is having unlimited limits on the above parameters.

    c. **Order Alerts and Reports –**Whether the system has capability to generate alerts when orders that are placed are above the limits and has capability to generate reports relating to Margin Requirements, payments and delivery obligations.

    d. **Order Review –**Whether the system has capability to facilitate review of such orders were not validated by the system.

    e. **Back testing for effectiveness of RMS –** Whether the system has capability to identify trades which have exceeded the pre-defined limits (Order Quantity and Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order Limit, Order Price limit) and also exceed corresponding margin availability of clients. Whether deviations from such pre-defined limits are captured by the system, documented and corrective steps taken.

f. **Log Management –** Whether the system maintains logs of alerts / changes / deletion / activation / deactivation of client codes and logs of changes to the risk management parameters mentioned above. Whether the system allows only authorized users to set the risk parameter in the RMS.

3. **Password Security**

a. **Organization Access Policy** – Whether the organization has a well documented policy that provides for a password policy as well as access control policy for the exchange provided terminals.

b. **Authentication Capability** – Whether the system authenticates user credentials by means of a password before allowing the user to login, and whether there is is a system for authentication of orders originating from Internet Protocol by means of two-factor authentication, including Public Key Infrastructure (PKI) based implementation of digital signatures.

c. **Password Best Practices –** Whether there is a system provision for masking of password, system prompt to change default password on first login, disablement of user id on entering multiple wrong passwords (as defined in the password policy document), periodic password change mandate and appropriate prompt to user, strong parameters for password, deactivation of dormant user id, etc.

4. **Session Management**

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.

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

c. **Inactive Session –** Whether the system allows for automatic trading session logout after a system defined period of inactivity.

d. **Log Management** – Whether the system generates and maintain logs of Number of users, activity logs, system logs, Number of active clients.

5. **Network Integrity**

a. **Seamless connectivity** – Whether stock broker has ensured that a backup network link is available in case of primary link failure with the exchange.

b. **Network Architecture –** Whether the web server is separate from the Application and Database Server.

c. **Firewall Configuration** – Whether appropriate firewall is present between stock broker's trading setup and various communication links to the exchange. Whether the firewall is appropriately configured to ensure maximum security.

6. **Access Controls**

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.

b. **Additional Access controls** – Whether the system provides for any authentication mechanism to access to various components of the exchange provided terminals. Whether additional password requirements are set for critical features of the system. Whether the access control is adequate.

7. **Backup and Recovery**

   a. **Backup and Recovery Policy –** Whether the organization has a well documented policy on periodic backup of data generated from the broking operations.

   b. **Log generation and data consistency** - Whether backup logs are maintained and backup data is tested for consistency.

   c. **System Redundancy –** Whether there are appropriate backups in case of failures of any critical system components.

8. **BCP/DR** (Only applicable for Stock Brokers having BCP / DR site)

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

   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).

   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.

   d. **Connectivity with other FMIs –** The system auditor should check whether there is an alternative medium to communicate with Stock Exchanges and other FMIs.

9. **Segregation of Data and Processing facilities –** 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.

10. **Back office data**

    a. **Data consistency –** The system auditor should verify whether aggregate client code data available at the back office of broker matches with the data submitted / available with the stock exchanges through online data view / download provided by exchanges to members.

    b. **Trail Logs –** The system auditor should specifically comment on the logs of Client Code data to ascertain whether editing or deletion of records have been properly documented and recorded and does not result in any irregularities.

11. **IT Infrastructure Management** (including use of various Cloud computing models such as Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS))

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.

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.

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.

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.

12. **Exchange specific exceptional reports –** The additional checks recommended by a particular exchange need to be looked into and commented upon by the system auditor over and above the ToR of the system audit.

Annexure II

ToR for Type II Broker

The system auditor shall at the minimum cover the following areas:

1. **System controls and capabilities (CTCL / IML terminals and servers)**

    a. **Order Tracking** – The system auditor should verify system process and controls at CTCL / IML terminals and CTCL/ IML servers covering order entry, capturing of IP address of order entry terminals, modification / deletion of orders, status of current order/outstanding orders and trade confirmation.

    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.

    c. **Rejection of orders –** Whether system has capability to reject orders which do not go through order level validation at CTCL servers and at the servers of respective stock exchanges.

    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.

    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.

    f. **Order type distinguishing capability –** Whether system has capability to distinguish the orders originating from (CTCL or IML) / IBT/ DMA / STWT.

2. **Software Change Management** - The system auditor should check whether proper procedures have been followed and proper documentation has been maintained for the following:

    a. Processing / approval methodology of new feature request or patches

    b. Fault reporting / tracking mechanism and process for resolution

    c. Testing of new releases / patches / modified software / bug fixes

    d. Version control- History, Change Management process , approval etc

    e. Development / Test / Production environment segregation.

    f. New release in production – promotion, release note approvals

    g. Production issues / disruptions reported during last year, reasons for such disruptions and corrective actions taken.

    h. User Awareness

    The system auditor should check whether critical changes made to the (CTCL or IML) / IBT / DMA / STWT/ SOR are well documented and communicated to the Stock Exchange.

3. **Risk Management System (RMS)**

a. **Online risk management capability –** The system auditor should check whether system of online risk management including upfront real-time risk management, is in place for all orders placed through (CTCL or IML) / IBT / DMA / STWT.

b. **Trading Limits –** Whether a system of pre-defined limits /checks such as Order Quantity and Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order Limit, Order Price limit, etc., are in place and only such orders which are within the parameters specified by the RMS are allowed to be pushed into exchange trading engines. The system auditor should check that no user or branch in the system is having unlimited limits on the above parameters.

c. **Order Alerts and Reports –** Whether the system has capability to generate alerts when orders that are placed are above the limits and has capability to generate reports relating to margin requirements, payments and delivery obligations.

d. **Order Review –** Whether the system has capability to facilitate review of such orders that were not validated by the system.

e. **Back testing for effectiveness of RMS –** Whether 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.

f. **Log Management –** Whether the system maintains logs of alerts / changes / deletion / activation / deactivation of client codes and logs of changes to the risk management parameters mentioned above. Whether the system allows only authorized users to set the risk parameter in the RMS.

4. **Smart order routing (SOR)** - The system auditor should check whether proper procedures have been followed and proper documentation has been maintained for the following:

a. **Best Execution Policy** – System adheres to the Best Execution Policy while routing the orders to the exchange.

b. **Destination Neutral –** The system routes orders to the recognized stock exchanges in a neutral manner.

c. **Class Neutral –** The system provides for SOR for all classes of investors.

d. **Confidentiality** - The system does not release orders to venues other than the recognized stock Exchange.

e. **Opt–out** – The system provides functionality to the client who has availed of the SOR facility, to specify for individual orders for which the clients do not want to route order using SOR.

f. **Time stamped market information** – The system is capable of receiving time stamped market prices from recognized stock Exchanges from which the member is authorized to avail SOR facility.

g. **Audit Trail -** Audit trail for SOR should capture order details, trades and data points used as a basis for routing decision.

h. **Server Location –** The system auditor should check whether the order routing server is located in India.

i. **Alternate Mode -** The system auditor should check whether an alternative mode of trading is available in case of failure of SOR Facility

5. **Password Security**

a. **Organization Access Policy** – Whether organization has a well documented policy that provides for a password policy as well as access control policy for exchange provided terminals and for API based terminals.

b. **Authentication Capability –** Whether the system authenticates user credentials by means of a password before allowing the user to login, and whether there is a system for authentication of orders originating from Internet Protocol by means of two-factor authentication, including Public Key Infrastructure (PKI) based implementation of digital signatures.

c. **Password Best Practices –** Whether there is a system provision for masking of password, system prompt to change default password on first login, disablement of user id on entering multiple wrong passwords (as defined in the password policy document), periodic password change mandate and appropriate prompt to user, strong parameters for password, deactivation of dormant user id, etc.

6. **Session Management**

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

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

c. **Inactive Session –** Whether the system allows for automatic trading session logout after a system defined period of inactivity.

d. **Log Management –** Whether the system generates and maintains logs of Number of users, activity logs, system logs, Number of active clients.

7. **Database Security**

a. **Access** – Whether the system allows CTCL or IML database access only to authorized users / applications.

b. **Controls –** Whether the CTCL or IML database server is hosted on a secure platform, with Username and password stored in an encrypted form using strong encryption algorithms.

8. **Network Integrity**

a. **Seamless connectivity –** Whether the stock broker has ensured that a backup network link is available in case of primary link failure with the exchange.

b. **Network Architecture –** Whether the web server is separate from the Application and Database Server.

c. **Firewall Configuration –** Whether appropriate firewall is present between stock broker's trading setup and various communication links to the exchange. Whether the firewall is appropriately configured to ensure maximum security.

9. **Access Controls**

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.

b. **Additional Access controls –** Whether the system provides for two factor authentication mechanism to access to various CTCL or IML components. Whether additional password requirements are set for critical features of the system. Whether the access control is adequate.

10. **Backup and Recovery**

a. **Backup and Recovery Policy –** Whether the organization has a well documented policy on periodic backup of data generated from the broking operations.

b. **Log generation and data consistency** - Whether backup logs are maintained and backup data is tested for consistency

c. **System Redundancy –** Whether there are appropriate backups in case of failures of any critical system components

11. **BCP/DR** (Only applicable for Stock Brokers having BCP / DR site)

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

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).

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.

d. **Connectivity with other FMIs –** The system auditor should check whether there is an alternative medium to communicate with Stock Exchanges and other FMIs.

12. **Segregation of Data and Processing facilities –** 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.

13. **Back office data**

a. **Data consistency –** The system auditor should verify whether aggregate client code data available at the back office of broker matches with the data submitted / available with the stock exchanges through online data view / download provided by exchanges to members.

b. **Trail Logs –** The system auditor should specifically comment on the logs of Client Code data to ascertain whether editing or deletion of records have been properly documented and recorded and does not result in any irregularities.

14. **User Management**

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.

b. **Access to Authorized users –** The system auditor should check whether the system allows access only to the authorized users of the CTCL or IML System. Whether there is a proper documentation of the authorized users in the form of User Application approval, copies of User Qualification and other necessary documents.

c. **User Creation / Deletion –** The system auditor should check whether new users ids were created / deleted as per CTCL or IML guidelines of the exchanges and whether the user ids are unique in nature.

d. **User Disablement –** The system auditor should check whether non-complaint users are disabled and appropriate logs (such as event log and trade logs of the user) are maintained.

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))

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.

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.

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.

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.

16. **Exchange specific exceptional reports –** The additional checks recommended by a particular exchange need to be looked into and commented upon by the System Auditor over and above the ToR of the System audit.

17. **Software Testing Procedures** - 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:
    a. **Test Procedure Review** – The system auditor should evaluate whether the procedures for system and software testing were proper and adequate.
    b. **Documentation** – The system auditor should verify whether the documentation related to testing procedures, test data, and resulting output were adequate and follow the organization's standards.
    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 SEBI.

Annexure III

ToR for Type III Broker

The system auditor shall at the minimum cover the following areas:

1. **System controls and capabilities (CTCL/IML Terminals and servers)**

    a. **Order Tracking** – The system auditor should verify system process and controls at CTCL / IML terminals and CTCL/ IML servers covering order entry, capturing IP address of order entry, modification / deletion of orders, status of current order/outstanding orders and trade confirmation.

    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.

    c. **Rejection of orders –** Whether the system has capability to reject orders which do not go through order level validation at CTCL servers and at the servers of respective exchanges.

    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.

    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.

    f. **Order type distinguishing capability –** Whether the system has capability to distinguish the orders originating from (CTCL or IML) / IBT / DMA / STWT / SOR / Algorithmic Trading.

2. **Software Change Management** - The system auditor should check whether proper procedures have been followed and proper documentation has been maintained for the following:

    a. Processing/approval methodology of new feature request or patches

    b. Fault reporting / tracking mechanism and process for resolution

    c. Testing of new releases / patches / bug fixes

    d. Version control- History, Change Management process , approval etc

    e. Development / Test/ Production environment segregation.

    f. New release in production – promotion, release note approvals

    g. Production issues/ disruptions reported during last year, reasons for such disruptions and corrective actions taken.

    h. User Awareness

    The System Auditor should check whether critical changes made to the (CTCL or IML) / IBT / DMA / STWT / SOR are well documented and communicated to the Stock Exchange.

3. **Risk Management System (RMS)**

a. **Online risk management capability –** The system auditor should check whether the online risk management including upfront real-time risk management, is in place for all orders placed through (CTCL or IML) / IBT/ DMA / SOR / STWT / Algorithmic Trading.

b. **Trading Limits –** Whether a system of pre-defined limits / checks such as Order Quantity and Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order Limit, Order Price limit, etc., are in place and only such orders which are within the parameters specified by the RMS are allowed to be pushed into exchange trading engines. The system auditor should check that no user or branch in the system is having unlimited limits on the above parameters.

c. **Order Alerts and Reports –** Whether the system has capability to generate alerts when orders that are placed are above the limits and has capability to generate reports relating to margin requirements, payments and delivery obligations.

d. **Order Review –** Whether the system has capability to facilitate review of such orders that were not validated by the system.

e. **Back testing for effectiveness of RMS –** Whether the system has capability to identify trades which have exceeded the pre-defined limits (Order Quantity and Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order Limit, Order Price limit) and also exceed corresponding margin availability of clients. Whether deviations from such pre-defined limits should be captured by the system, documented and corrective steps taken.

f. **Log Management –** Whether the system maintains logs of alerts / changes / deletion / activation / deactivation of client codes and logs of changes to the risk management parameters mentioned above. Whether the system allows only authorized users to set the risk parameter in the RMS.

4. **Smart order routing (SOR)** - The system auditor should check whether proper procedures have been followed and proper documentation has been maintained for the following:

a. **Best Execution Policy** – System adheres to the Best Execution Policy while routing the orders to the exchange.

b. **Destination Neutral –** The system routes orders to the recognized stock exchanges in a neutral manner.

c. **Class Neutral –** The system provides for SOR for all classes of investors.

d. **Confidentiality** - The system does not release orders to venues other than the recognized stock Exchange.

e. **Opt–out** – The system provides functionality to the client who has availed of the SOR facility, to specify for individual orders for which the clients do not want to route order using SOR.

f. **Time stamped market information** – The system is capable of receiving time stamped market prices from recognized stock Exchanges from which the member is authorized to avail SOR facility.

g. **Audit Trail -** Audit trail for SOR should capture order details, trades and data points used as a basis for routing decision.

h. **Server Location –** The system auditor should check whether the order routing server is located in India.

i. **Alternate Mode -** The system auditor should check whether an alternative mode of trading is available in case of failure of SOR Facility

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

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

   b. **Online Risk Management capability-** The CTCL or IML server should have capacity to monitor orders / trades routed through algo trading and have online risk management for all orders through Algorithmic trading and ensure that Price Check, Quantity Check, Order Value Check, Cumulative Open Order Value Check are in place.

   c. **Risk Parameters Controls –** The system should allow only authorized users to set the risk parameter. The System should also maintain a log of all the risk parameter changes made.

   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.

   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.

   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.

   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.

   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.

i. **Reporting to Stock Exchanges –** The system auditor should check whether the stock broker is informing the stock exchange regarding any incidents where the algos have not behaved as expected. The system auditor should also comment upon the time taken by the stock broker to inform the stock exchanges regarding such incidents.

6. Password Security

a. **Organization Access Policy** – The system auditor should whether the stock broker has a well documented policy that provides for a password policy as well as access control policy for exchange provided terminals and for API based terminals.

b. **Authentication Capability –** Whether the system authenticates user credentials by means of a password before allowing the user to login. 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.

c. **Password Best Practices –** Whether there is a system should 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.

7. Session Management

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.

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

c. **Inactive Session –** Whether the system allows for automatic trading session logout after a system defined period of inactivity.

d. **Log Management –** Whether the system generates and maintains logs of number of users, activity logs, system logs, number of active clients.

8. Database Security

a. **Access –** Whether the system allows CTCL or IML database access only to authorized users / applications.

b. **Controls –** Whether the CTCL or IML database server is hosted on a secure platform, with username and password stored in an encrypted form using strong encryption algorithms.

9. Network Integrity

a. **Seamless connectivity –** Whether the stock broker has ensured that a backup network link is available in case of primary link failure with the exchange.

b. **Network Architecture –** Whether the web server is separate from the Application and Database Server.

c. **Firewall Configuration –** Whether appropriate firewall are present between the stock broker's trading setup and various communication links to the exchange. Whether the firewalls should be appropriately configured to ensure maximum security.

10. Access Controls

a. **Access to server rooms –** Whether adequate controls are in place for access to server rooms, proper audit trails should be maintained for the same.

b. **Additional Access controls -** Whether the system should provide for two factor authentication mechanism to access to various CTCL or IML components. Whether additional password requirements are set for critical features of the system. Whether the access control is adequate.

11. Backup and Recovery

a. **Backup and Recovery Policy –** Whether the organization has a well documented policy on periodic backup of data generated from the broking operations.

b. **Log generation and data consistency** – Whether backup logs are maintained and backup data should be tested for consistency.

c. **System Redundancy –** Whether there are appropriate backups in case of failures of any critical system components.

12. BCP/DR (Only applicable for Stock Brokers having BCP / DR site)

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

b. **Alternate channel of communication –** Whether the stock broker has provided its clients with alternative 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).

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.

d. **Connectivity with other FMIs –** The system auditor should check whether there is an alternative medium to communicate with Stock Exchanges and other FMIs.

13. Segregation of Data and Processing facilities – 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.

14. Back office data

a. **Data consistency –** The system auditor should verify whether aggregate client code data available at the back office of broker matches with the data submitted / available with the stock exchanges through online data view / download provided by exchanges to members.

b. **Trail Logs –** The system auditor should specifically comment on the logs of Client Code data to ascertain whether editing or deletion of records have been properly documented and recorded and does not result in any irregularities.

15. User Management

a. **User Management Policy –** The system auditor should verify 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.

b. **Access to Authorized users –** The system auditor should verify whether the system allows access only to the authorized users of the CTCL or IML system. Whether there is a proper documentation of the authorized users in the form of user application approval, copies of user qualification and other necessary documents.

c. **User Creation / Deletion –** The system auditor should verify whether new users ids should be created / deleted as per CTCL or IML guidelines of the exchanges and whether the user ids are unique in nature.

d. **User Disablement –** The system auditor should verify whether non-complaint users are disabled and appropriate logs such as event log and trade logs of the user should be maintained

16. 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))

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.

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.

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.

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.

17. **Exchange specific exceptional reports –** The additional checks recommended by a particular exchange need to be looked into and commented upon by the system auditor over and above the ToR of the system audit.

18. **Software Testing Procedures** - The system auditor shall audit 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:

    a. **Test Procedure Review** – The system auditor should review and evaluate the procedures for system and program testing. The system auditor should also review the adequacy of tests.

    b. **Documentation** – The system auditor should review documented testing procedures, test data, and resulting output to determine if they are comprehensive and if they follow the organization's standards.

    c. **Test Cases** – The system auditor should review the test cases and comment upon the adequacy of the same with respect to the requirements of the Stock Exchange anld various SEBI Circulars.

Annexure -IV

Executive Summary Reporting Format

I. For Preliminary Audit

Audit Date	Observation No	Description of Finding	Department	Status / Nature of Findings	Risk Rating of Findings	Audit TOR Clause	Audited By	Root Cause Analysis	Impact Analysis	Suggested Corrective Action	Deadline for the Corrective Action	Verified By	Closing Date

Description of relevant Table heads

1. **Audit Date –** This indicates the date of conducting the audit.
2. **Description of Findings/ Observations –** Description of the findings in sufficient detail, referencing any accompanying evidence (e.g. copies of procedures, interview notes, screen shots *etc*.)
3. **Status/ Nature of Findings -** the category can be specified for example:
    a. Non Compliant
    b. Work In progress
    c. Observation
    d. Suggestion

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

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

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

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

II. For Follow on / Follow up System Audit

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

Description of relevant Table heads

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