Terms of Reference (ToR) - II

Sr. no.	Particulars
1	**System controls and capabilities(IML terminals and servers)**
a.	**Order Tracking –** The system auditor should verify system process and controls at IML terminals and 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 IML 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 IML / IBT/ DMA / STWT.
2	**Software Change Management - The system auditor should check whether critical changes made to the IML / IBT / DMA / STWT/ SOR are well documented and communicated to the Stock Exchange. 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
i.	Changes undertaken pursuant to a change to the stock Exchange's trading system
j.	Adequate mechanism for restoration of trading systems to production state at the end of testing session so as to ensure integrity of stock broker's trading system

Terms of Reference (ToR) - II

Sr. no.	Particulars
k.	The auditor should check that stock brokers are not using software without requisite approval of stock Exchange and there has not been any unauthorized change to the approved software
3	**Risk Management System (RMS)**
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 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.

Terms of Reference (ToR) - II

Sr. no.	Particulars
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.	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.	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.

Terms of Reference (ToR) - II

Sr. no.	Particulars
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 IML database access only to authorized users / applications.
b.	**Controls –** Whether the 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 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.

Terms of Reference (ToR) - II

Sr. no.	Particulars
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.	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 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 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.

Terms of Reference (ToR) - II

Sr. no.	Particulars
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.	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

Terms of Reference (ToR) - II

Sr. no.	Particulars
d.	**Testing of software**: The system auditor should verify whether member has complied with the process for testing of their new/modified software as prescribed by SEBI vide its circular dated August 19, 2013 and February 7, 2014 regarding testing in (i)Simulated test environment (ii) Mock testing (iii) User Acceptance testing(UAT)
18	**Whether the stock broker has quarterly intimated to the stock Exchange as per SEBI circular no. SEBI/HO/MIRSD/DOS2/CIR/P/2019/10 dated January 4, 2019 regarding use of AI(Artificial Intelligence) and ML(Machine Language) application and systems.**
19	**Implementation of a) Recommendations in previous system audit report and b) Action Taken in case of medium / weak areas in reports submitted for prior approval.**
a.	The System auditor should verify the observations / issues / recommendations mentioned in the previous system audit report and cover open items in the report and specify whether the member has implemented those observations / issues / recommendations/ open items. If not, provide the reasons for not implementation .
b.	The System auditor should verify if member have been rated as "Medium/Weak" in any areas by System auditor during audit period (prior to granting approval for Internet based Trading/ Direct Market Access/ SOR/ Wireless securities trading) please provide action taken by member on these areas .
20	Comments of the auditor on any other area