Master Circular for Broker Dealers and Clearing Members

Table of Contents

CHAPTER – I: PROCESS OF REGISTRATION

1. Application for Registration

1.1 IFSCA has operationalised a Single Window IT System (SWIT System/ SWITS), which, inter-alia, contains a Common Application Form (CAF), created by merging several existing forms including business-specific Annexure Forms.

1.2 The link for accessing the SWITS platform is https://swit.ifsca.gov.in.

1.3 The SWIT System aims to harmonise and simplify the process of submission of application under the Acts specified under the First Schedule of the IFSCA Act, 2019, including any regulations or framework issued thereunder, in addition to the Special Economic Zones (SEZ) Act, 2005. The Application Form (Form-FA) for seeking Letter of Approval (LoA) from the Administrator (IFSCA) under the SEZ Act, 2005 is also the part of the SWITS and is integrated with the SEZ Online System.

1.4 In addition, the SWIT System also integrates within itself a No objection Certificate (NOC) processing module that eases the process for obtaining an NOC, wherever necessary, from the appropriate regulators viz. RBI, SEBI or IRDAI. For example, for an entity which is registered with SEBI, an NOC from SEBI can be obtained through the SWIT System.

1.5 In addition, the SWIT System also provides the facility for an entity to apply for Goods and Services Tax Identification Number (GSTIN), thereby simplifying the tax registration for businesses.

1.6 Further, the SWIT System also enables the online payment of fees in USD for entities desirous of setting up operations in IFSC.

1.7 An entity desirous of seeking registration as a Broker Dealer or Clearing Member with the International Financial Services Centres Authority (IFSCA / the Authority) shall submit/file its applications exclusively through the SWIT System for seeking:

1.7.1 Registration as Broker Dealer or Clearing Member under the provisions of the IFSCA (Capital Market Intermediaries) Regulations, 2025 (CMI Regulations). Such application shall be submitted to IFSCA through respective Stock Exchange/Clearing Corporation

1.7.2 Approvals from SEZ Authorities and GST registration

1.7.3 NoC/requisite approval from appropriate regulators

1.8 For more details, please refer to the circular titled "Single Window IT System inter-alia for registration and approval from IFSCA, SEZ authorities, GSTN, RBI, SEBI and IRDAI" issued by IFSCA on September 30, 2024 in this regard.

2. **Payment of Fees**

2.1 An applicant seeking registration as Broker Dealer or Clearing Member under the CMI Regulations shall pay the application fee, as specified in Schedule-I of the circular titled "Fee structure for the entities undertaking or intending to undertake permissible activities in IFSC or seeking guidance under the Informal Guidance Scheme" ("IFSCA Fee Circular") dated April 08, 2025, read with circular titled "Clarifications on the Fee structure for the entities undertaking or intending to undertake permissible activities in IFSC or seeking guidance under the Informal Guidance Scheme" dated April 23, 2025, at the time of making an application to the Authority. If an application is not accompanied by the mandated application fee, such an application shall not be considered by the Authority.

2.2 On intimation of the decision by the Authority to grant an in-principle approval, the applicant shall, within 15 days of such an intimation, pay the applicable registration fees as specified in Schedule-I of the IFSCA Fee Circular.

2.3 In those cases where the applicant fails to pay the requisite registration fees within the specified time, it shall be presumed that the applicant does not wish to continue the process. In such a case, the Authority may at its discretion reject the application. An application once rejected, shall be treated as non-est. The rejection of the application, however, shall not render the entity ineligible for making a fresh application.

2.4 In case the Authority decides not to grant registration to an applicant to whom a provisional / in-principle approval has been granted, the fees paid by the applicant towards obtaining licence, registration, recognition or authorization fee shall not be refunded.

2.5 The fees as specified in the Schedule-I of the IFSCA Fee Circular shall be paid to the following account of the Authority in USD:

Account Name: International Financial Services Centres Authority

Account Number: 970105000174
Type of Account: USD Current Account
Bank Name: ICICI Bank Limited
SWIFT Code: ICICINAAXXX
NOSTRO Details: CHASUS33XXX
JP MORGAN CHASE BANK NA, NEWYORK, USA
Account no: 833999532

2.6 An applicant from India (other than an entity already set up in IFSC) desirous of getting registration from the Authority shall have the option to pay only the application fee and registration fee, as specified in the Schedule-I of the IFSCA Fee Circular, in INR into the following account of the Authority:

Account Name: IFSCA FUND 2
Account Number: 39907189884
Name of the Bank: State Bank of India
Type of Account: INR Current Account
IFSC Code: SBIN0060228

2.7 For the entities remitting the fees in INR, the RBI reference rate for USD-INR, for the date on which the remittance is being made, shall be applicable. The RBI reference rate is available at the URL:

https://www.rbi.org.in/scripts/ReferenceRateArchive.aspx

2.8 The applicable fee shall be paid in full, as indicated in Schedule-I of the IFSCA Fee Circular, net of any deductions or charges. All applicable charges towards remittance of the amount, shall be borne by the applicant/ Broker Dealer/ Clearing Member.

2.9 After the payment of the applicable fees, the applicant / Broker Dealer/ Clearing Member shall submit the documentary evidence of such a payment to the Authority, along with the details of such payment in the form and manner specified at Schedule-II of the IFSCA Fee Circular.

2.10 All dues or fees payable to the Authority shall be paid by the applicant / Broker Dealer/ Clearing Member either from the bank account of the entity or that of its KMPs. In case the payment has been made from the account of the KMPs, the same shall be informed to the Authority during submission of the documentary evidence. However, in case of an initial payment of application and registration fee, such amount can be paid either by the parent or the promoter of the applicant.

2.11 A Broker Dealer or Clearing Member registered or Authorised with the Authority shall pay annual fee and other applicable fees in accordance with the IFSCA Fee Circular.

3. Validity of Registration

3.1 The certificate of registration granted to a Broker Dealer or Clearing Member shall be perpetual, unless it is suspended or cancelled by the Authority.

3.2 The Broker Dealer or Clearing Member shall always ensure that it holds valid and subsisting

3.2.1 Certificate of Registration issued by the Authority under the CMI Regulations; and

3.2.2 Letter of Approval (LoA) under the Special Economic Zones Act, 2005.

3.3 It may also be noted that the expiry of the Letter of Approval (having validity of 1 year, if business not commenced; or 5 years, after commencement of business) or failure to renew it in a timely manner, may lead to appropriate enforcement action, including cancellation of the registration granted under the CMI Regulations.

3.4 The Broker Dealer or Clearing Member shall ensure compliance with the Circular titled "Direction for all Regulated Entities" dated April 03, 2025, issued by the Authority.

CHAPTER – II: SUPERVISION & OVERSIGHT

4. Oversight of Broker Dealers or Clearing Members

4.1 Inspection of Members by Stock Exchanges / Clearing Corporations

4.1.1 The Stock Exchange and the Clearing Corporation shall formulate a policy for inspection of their members and follow up action thereon. The policy shall also cover various kinds of risks posed to the investors and market at large on account of the activities/business conduct of their members.

4.1.2 The Stock Exchange and the Clearing Corporation shall conduct inspection of their members in terms of the above policy and in case of members who hold multiple memberships of the exchanges, the Stock Exchanges shall establish an information sharing mechanism with one another on the important outcome of inspection in order to improve the effectiveness of supervision.

4.1.3 The inspection shall cover:

a) Compliance with the relevant provisions of the Act, Rules and Regulations made there under, Rules and Regulation of the Stock Exchange / Clearing Corporation and the circulars issued by IFSCA and Stock Exchanges / Clearing Corporations from time to time, and

b) Efficacy of the investor grievance redressal mechanism and discharge of various obligations towards clients, for the preceding one year unless a longer period is warranted in the circumstances.

4.1.4 The Stock Exchange or the Clearing Corporation, as the case may be, shall initiate all the follow up action – remedial, penal and disciplinary - required on inspection findings, within six months from the conclusion of the inspection.

4.1.5 The clearing activity undertaken by a Broker Dealer for other Broker Dealers shall be inspected by the Clearing Corporation. Other activities of Broker Dealers shall be inspected by Stock Exchanges. If the Stock Exchanges and Clearing Corporations so desire, they may conduct joint inspections of Broker Dealers.

4.1.6 The Stock Exchange(s) and Clearing Corporation(s) can also conduct joint inspection with other Stock Exchange(s) and Clearing Corporation(s).

4.1.7 The Stock Exchanges/Clearing Corporations are advised to continuously assess the risks posed by their members and review/revise the policy of annual inspection, as and when required.

4.1.8 The Stock Exchanges shall establish an information sharing mechanism with one another on the important outcome of inspection of members who hold multiple memberships of the exchanges in order to improve the effectiveness of supervision and shall also bring cases of repetitive and / or serious violations to the notice of IFSCA.

4.2 Monitoring of Clients' Funds lying with the Broker Dealer by the Stock Exchanges

4.2.1 The Stock Exchanges in IFSC shall put in place a mechanism for monitoring clients' funds lying with the Broker Dealers.

4.3 Standard Operating Procedures for Broker Dealers - Actions to be contemplated by Stock Exchanges for any event-based discrepancies

4.3.1 Stock Exchanges and Clearing Members shall frame various event-based monitoring criteria based on market dynamics and market intelligence for monitoring of Broker Dealers. An illustrative list of such monitoring criteria are given below:

A. Monitoring criteria for Broker Dealers and Clearing Members

a. Failure to furnish net worth certificate to Stock Exchange / Clearing Corporation within the timeline specified by the Stock Exchange / Clearing Corporation.

b. Failure to furnish Annual Compliance Audit Report to Stock Exchange / Clearing Corporation / IFSCA as required under the regulation 25 (2) of the CMI Regulations.

c. Failure to furnish Annual Audited Accounts to the Stock Exchange / Clearing Corporation.

d. Failure to co-operate with the Stock Exchange / Clearing Corporation for the inspection related proceedings.

e. Failure to submit any other information within the specified timeline.

f. Failure to report new accounts opened by the Broker Dealer to exchanges within the time specified for reporting of such accounts.

4.3.2 With respect to net worth it is clarified (IFSCA circular dated September 05, 2024 on "Maintenance of Net Worth by Capital Market Intermediaries" may please be referred) that a Broker Dealer / Clearing Member failing to maintain Net Worth at any time shall not undertake any existing or new business activity in IFSC till the time the net worth is restored.

5. Running Account Settlement

5.1 Unless otherwise specified by IFSCA, settlement of funds shall be done as per the Agreement/Consent Letter between the Broker Dealer and its client. The Stock Exchanges in IFSC may specify the format of such Agreement/ Consent Letter for the Broker Dealers.

5.2 Such an Agreement/Consent Letter needs to be executed between the Broker Dealer and the Client at the time of onboarding itself.

5.3 In case of existing clients, the Broker Dealers in IFSC may adopt a procedure to operationalize the same.

5.4 The Stock Exchanges in IFSC shall put in place a mechanism for monitoring clients' funds lying with the Broker Dealers.

6. System Audit of Broker Dealers

6.1. The guidelines for the system audit of Broker Dealers prescribed below includes System Audit Process, Auditor Selection Norms and Terms of Reference (TOR).

6.2. The Stock Exchanges shall ensure that system audit of Broker Dealers is conducted in accordance with the prescribed guidelines.

6.3. The Stock Exchanges are advised to keep track of findings of system audits of all Broker Dealers on quarterly basis and ensure that all major audit findings, specifically in critical areas, are rectified / complied in a time bound manner failing which follow up inspection of such Broker Dealers may be taken up for necessary corrective steps / actions thereafter, if any.

6.4. The Stock Exchange shall report all major non-compliances / observations of system auditors, broker wise, on a quarterly basis to IFSCA.

6.1 Audit Process

6.1.1 The system audit of Broker Dealers shall be conducted with the following periodicity:

6.1.1.1 Annual system audit is to be done for all the Broker Dealers

6.1.1.2 Half yearly system audit is to be done for Broker Dealers who use Algorithmic Trading or provide their clients with the facility of Algorithmic Trading.

6.1.2 Such an audit shall be conducted in accordance with the Norms, Terms of Reference (ToR) and Guidelines issued by IFSCA and / or by Stock Exchanges. Separate ToRs are specified for the following categories of Broker Dealers:

6.1.2.1 Type I

Broker Dealers who trade through exchange provided terminals such as NEAT, BOLT etc. (ToR attached as **Annexure-1**);

6.1.2.2 Type II

Broker Dealers 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 Broker Dealers. (ToR attached as **Annexure-2**)

6.1.2.3 Type III

Broker Dealers who use Algorithmic Trading facility to trade and who may also be TYPE II Broker Dealers. (ToR attached as **Annexure-3**)

6.1.3 The Broker Dealers shall select auditors as per the selection norms provided in the guidelines and directions issued by Stock Exchanges and IFSCA from time to time. The Auditor may perform an audit of the Broker Dealer for a maximum period of three years.

6.1.4 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 Broker Dealers and directions issued by IFSCA from time to time in this regard.

6.1.5 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 be forwarded to the Stock Exchange by the Broker Dealer along with management comments, within one month of submission of report by the auditor.

6.1.6 The Stock Exchange shall ensure that the senior management of the Broker Dealer provides their comments 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 shall indicate if a follow-on audit is required to review the status of NCs.

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

6.1.8 The system auditors shall follow the reporting standard as specified in **Annexure-4** of this Framework for the executive summary of the

System Audit report to highlight the major findings of the System Audit.

6.2 Auditor Selection Norms

6.2.1 The Auditor shall have minimum three years of experience in IT audit of securities market participants e.g. Stock Exchanges, Clearing Corporation, Depositories, Broker Dealers, depository participants etc. The audit experience should cover all the major areas mentioned under Terms of Reference (ToR) of the system audit specified by IFSCA / Stock Exchange.

6.2.2 It is recommended that resources employed shall have relevant industry recognized certifications such as, but not limited to :

- 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^2)

6.2.3 The Auditor is required have the requisite experience of IT audit/governance frameworks and processes conforming to industry leading practices like Control Objectives for Information and Related Technologies (COBIT).

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

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

7. Early Warning Mechanism to Prevent Diversion of Client Securities

7.1 It has been decided to put in place an Early Warning Mechanism and sharing of information between Stock Exchanges, Depositories and Clearing Corporations

to detect the diversion of client's securities by the Broker Dealer at an early stage so as to take appropriate preventive measures. The threshold for such early warning signals shall be decided by the Stock Exchanges, Depositories and Clearing Corporations with mutual consultation.

CHAPTER III – DEALING WITH CLIENT

8. Unique Client Code

8.1 It shall be mandatory for the broker to use unique client code for all clients.

9. Regulation of Transactions Between Clients and Broker Dealers

9.1. It shall be compulsory for all Broker Dealers to keep the money of the clients in a separate account and their own money in a separate account. No payment for transactions in which the Member broker is taking a position as a principal will be permitted to be made from the client's account.

9.2. Broker Dealers shall issue the contract note for purchase/sale of securities to a client within 24 hours of the execution of the contract.

9.3. Broker Dealers should have adequate systems and procedures in place to ensure that client collateral is not used for any purposes other than meeting the respective client's margin requirements / pay-ins. Broker Dealers should also maintain records to ensure proper audit trail of use of client collateral.

9.4. Rule 8(1)(f) and Rule 8(3)(f) of the SCRR 1957, requires that members of a Stock Exchange, shall not engage in any business other than that of securities. Stock Exchanges shall ensure that the Broker Dealers are compliant with the requirements of the SCRR.

9.5. The Broker Dealer shall disclose to its Clients whether it conducts proprietary trading in conjunction with client-based business. To ensure complete transparency, this disclosure shall be made upfront at the time the Know Your Client (KYC) agreement is formalized.

10. Market Access through Authorised Persons in foreign jurisdictions

10.1. The Broker Dealers are permitted to provide market access to investors through Authorized Persons based in foreign jurisdictions.

11. Market Access through Authorised Persons in India

11.1. Further to enable access to resident Indian investors through Liberalized Remittance Scheme (LRS) route, for exchange traded securities in IFSC, it has been decided to permit IFSCA registered Broker Dealers to provide market access to investors through Authorized Persons based in India.

11.2. The regulatory framework governing the market access through Authorized Persons is enclosed at **Annexure-5**.

CHAPTER IV – TECHNOLOGY RELATED PROVISIONS

12. Electronic Contract Note (ECN)

12.1. The Broker Dealers are permitted to issue contract notes authenticated by means of digital signatures provided that the Broker Dealer has obtained the digital signature certificate from a Certifying Authority under the Information and Technology Act, 2000.

13. Testing of software used in or related to trading and Risk Management

13.1. The term 'software' shall mean electronic systems or applications used by Broker Dealers / trading members for connecting to the Stock Exchanges and for the purposes of trading and real-time risk management, including software used for:

- Internet Based Trading (IBT),
- Direct Market Access (DMA),
- Securities Trading using Wireless Technology (STWT),
- Smart Order Routing (SOR),
- Algorithmic Trading (AT), etc.

13.2. Testing of Software

13.2.1. The Stock Exchanges shall frame appropriate testing policies for functional as well as technical testing of the software. Such framework shall at the minimum include the following:

a. Testing in a simulated test environment

The Stock Exchanges shall provide suitable facilities to market participants / software vendors to test new software or existing software that have undergone change. Subjecting the new software or existing software that have undergone change to such testing facility shall be mandatory for market participants, before putting it in use.

b. Mock testing

i. The Stock Exchanges shall organize mock trading sessions on regular basis, at least once in a calendar month, to facilitate testing of new software or existing software that has undergone any change of functionality, in a close-to-real trading environment. The Stock Exchanges shall suitably design and plan such mock trading sessions to ensure maximum participation and sufficient trading volumes for the purpose of testing.

ii. The Stock Exchanges shall mandate a minimum time period for such testing in the mock trading sessions.

iii. In order to improve the efficacy of the mock trading sessions, all Broker Dealers shall ensure that all userids approved for Algo trading, irrespective of the algorithm having undergone change or not, shall participate in the mock trading sessions.

iv. The requirement of mandatory mock trading sessions to facilitate testing of new software or existing software that has undergone any change of functionality shall be optional if a Stock Exchange provides suitable simulated test environment to test new software or existing software that has undergone any change of functionality and ensures the following:

    i. The test environment shall be made available to all the members.

    ii. The test environment shall be made available for at least two hours after market hours and at least on two trading days in a week.

    iii. For the purpose of testing, the Stock Exchange shall make available data from at least one trading day and the same shall not be older than one month from the day of the testing environment.

    iv. All Broker Dealers (excluding those who use only Exchange provided front end and/or ASP services) having approved Algorithms available with the Broker Dealer, irrespective of the algorithm having undergone change or not, shall participate in the Simulated Environment at least on one trading day

during each calendar month at all the exchanges where they are members. This shall be audited and reported in the System Auditors report.

c. User Acceptance Test (UAT): The Broker Dealer shall undertake UAT of the software to satisfy itself that the newly developed / modified software meets its requirements.

d. With respect to testing of software related to (i) fixes to bugs in the software, (ii) changes undertaken to the Broker Dealers' software / systems pursuant to a change to any Stock Exchange's trading system, and (iii) software purchased from a software vendor that has already been tested in the mock environment by certain number of Broker Dealers, Stock Exchanges may prescribe a faster approval process to make the process of approval expeditious.

13.2.2. The Broker Dealers shall also engage system auditor(s) to examine reports of mock tests and UAT in order to certify that the tests were satisfactorily undertaken.

13.2.3. The Stock Exchanges shall monitor the compliance of Broker Dealers, who use trading algorithms, with regard to the requirement of participation in mock trading session as mandated herein. In those cases where the Stock Exchanges find that the Broker Dealer has failed to participate in such mock trading sessions, the Stock Exchange shall call for reasons and if found unsatisfactory, shall suspend the proprietary trading rights of the Broker Dealer for a minimum period of one trading day.

13.2.4. The Stock Exchanges shall also ensure that the system auditors examine the compliance of Broker Dealer, who use trading algorithms, with regard to the requirement of participation in mock trading session, as mandated herein, and provide suitable comments in the periodic system audit report. In cases where the system audit report indicate that the Broker Dealer has failed to participate in such mock trading sessions, Stock Exchange shall call for reasons from the Broker Dealer and if found unsatisfactory, shall suspend the proprietary trading rights of the Broker Dealer for a minimum period of one trading day.

13.2.5. For pre-approval / periodic system audit of Computer-to-Computer Link (CTCL) or Intermediate Messaging Layer (IML), IBT, DMA, STWT, SOR and AT, Broker Dealers shall engage a system auditor with any of the certifications specified by the IFSCA. While finalizing the system auditor, Broker Dealers

shall ensure the system auditor does not have any conflict of interest with the Broker Dealer and the directors / promoters of the system auditor are not directly or indirectly related to the current directors or promoters of Broker Dealer.

13.3. Approval of Software of Broker Dealer

13.3.1. Broker Dealers shall seek approval of the respective Stock Exchanges for deployment of the software in the securities market by submitting necessary details required by Stock Exchange including details of software, tests undertaken and certificate / report provided by the system auditor. Stock Exchange may seek additional details as deemed necessary for evaluating the application of the Broker Dealer.

13.3.2. The Stock Exchanges shall grant approval or reject the application of the Broker Dealer as the case may be and communicate the decision to the Broker Dealer within fifteen working days from the date of receipt of completed application (or within any other such time period specified by the IFSCA). In case of rejection of the application, the Stock Exchange shall also communicate reasons of rejection to the Broker Dealer within such time period.

13.3.3. Before granting approval to use software in securities market, Stock Exchange shall ensure that the requirements specified by IFSCA / Stock Exchange with regard to software are met by the Broker Dealer.

13.3.4. The Stock Exchanges may suitably schedule the requirements of mock testing, certification of test reports by system auditor(s) and the software approval process, so as to facilitate a speedy approval and a smooth transition of the Broker Dealers to the new / upgraded software.

13.3.5. In order to ensure that Broker Dealers are not using software without requisite approval, The Stock Exchanges are advised to put in place suitable mechanism to prevent any unauthorized change to the approved software.

13.4. Undertaking to be provided by Broker Dealers

13.4.1. Broker Dealers shall submit an undertaking to the respective Stock Exchanges stating the following at the minimum:

a. M/s (name of the Broker Dealer) 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 IFSCA / Stock Exchange before deployment of such new / modified software in securities market.

b. M/s (name of the Broker Dealer) will ensure that approval of the Stock Exchange is sought for all new / modified software and will comply with various requirements specified by IFSCA or the Stock Exchange from time to time with regard to usage, testing and audit of the software.

c. The absolute liability arising from failure to comply with the above provisions shall lie entirely with M/s (name of the Broker Dealer)

13.4.2. The Stock Exchanges may include additional clauses as deemed necessary in the undertaking.

13.5. Sharing of Application Programming Interface (API) specifications by the Stock Exchange with Broker Dealers:

13.5.1. API is an interface that enables interaction of software with other software and typically includes language and message format that is used by an application program to communicate with the operating system or other application program. Broker Dealers and software vendors require relevant API specifications to facilitate interaction of the developed software with the systems of the Stock Exchanges.

13.5.1.1. The Stock Exchanges shall provide relevant API specifications to all Broker Dealers and software vendors who are desirous of developing software for the securities market, after establishing their respective credentials.

13.5.1.2. In case of refusal to share APIs, The Stock Exchanges shall provide reasons in writing to the desirous Broker Dealers or software vendors within a period of fifteen working days from the date of receipt of such request for sharing of API.

13.5.1.3. Further, The Stock Exchanges shall not selectively release updates / modifications, if any, of the existing API specifications to few Broker Dealers or software vendors ahead of others and shall provide such updated / modified API specifications to all Broker Dealers and software vendors with whom the earlier API specifications were shared.

13.6. Penalty on malfunction of software used by Broker Dealer

13.6.1. The Stock Exchanges shall examine the cases of malfunctioning of software used by Broker Dealers and apply deterrent penalties in form of fines or suspension to the Broker Dealer whose software malfunctioned. In addition, Broker Dealers shall implement various mechanisms including the following to minimize their losses in the event of software malfunction:

13.6.1.1. include suitable clauses in their agreement with the software vendors to define liabilities of software vendor and Broker Dealer / trading member in case of software malfunction, and / or,

13.6.1.2. consider taking suitable insurance cover to meet probable losses in case of software malfunction.

13.6.2. With regard to changes / updates to Broker Dealers' trading software that intend to modify the 'look and feel' and do not affect the risk management system of the Broker Dealer or the connectivity of the trading software with Stock Exchange's trading system, it is clarified that mock testing and consequent system audit may not be insisted upon by the Stock Exchanges.

13.6.3. The Stock Exchanges shall direct their Broker Dealers to put in place adequate mechanism to restore their trading systems to 'production state' at the end of testing session so as to ensure integrity of Broker Dealers' trading system.

14. Safeguards to avoid trading disruption in case of failure of Software Vendor

14.1. Software vendors who provide software to market participants and market infrastructure institutions for the purpose of trading, risk management, clearing and settlement play a crucial role in the securities market. Any inability on the part of such software vendors to provide software or related services in timely and continuous manner may create a situation of stress in the securities market.

14.2. Adequate mechanism / procedure should be in place to ensure smooth transition by Broker Dealer(s) to another software vendor in case of inability of the existing software vendor to provide software and related services in timely and continuous manner.

14.3. The Stock Exchanges may advise the Broker Dealers to take the following measures:

14.3.1. Explore the possibility of establishing a 'software escrow arrangement' with their existing software vendors.

14.3.2. In case of large Broker Dealers, consider reducing dependence on a single software vendor for trading and risk management systems, by engaging more than one software vendor.

14.3.3. Consider including the following in their contracts with the software vendors:

a. access to documents related to design and development specifications in the event software vendor fails to provide continuous and timely services to the Broker Dealer;

b. development of expertise at the end of the Broker Dealer through appropriate training with regard to software usage and maintenance;

c. appropriate penalty clauses for cases of disruptions to the trading system of the Broker Dealer on account of (i) software vendor failing to provide continuous and timely services to the Broker Dealer or (ii) glitches to the software provided by the software vendor;

d. obligation on the part of the software vendor to cooperate in case of audit of software including forensic audit, if required.

15. Cyber Security and Cyber Resilience

15.1. In terms of regulation 21 of the CMI Regulations, the Broker Dealer or Clearing Member shall have robust cyber security and cyber resilience framework in accordance with the requirements as may be specified by the Authority.

15.2. The Broker Dealer or Clearing Member shall comply with the guidelines specified under the circular titled "Guidelines on Cyber Security and Cyber Resilience for Regulated Entities in IFSCs" dated March 10, 2025.

15.3. As mentioned in the said circular, the implementation of these Guidelines shall be undertaken in accordance with the principle of proportionality, after taking into due consideration:

15.3.1. the scale and complexity of operations
15.3.2. the nature of the activity the entity is engaged in,
15.3.3. its interconnectedness with the financial ecosystem and
15.3.4. the corresponding cyber risks the entity is exposed to.

16. Reporting for Artificial Intelligence (AI) and Machine Learning (ML) applications and systems offered and used by market intermediaries

16.1. All registered Broker Dealers offering or using AI and ML systems shall make the requisite reporting to the Stock Exchanges in such a manner and form as specified by the Stock Exchanges.

17. Framework to address the 'technical glitches' in Broker Dealers' Electronic Trading Systems

17.1. Technology related interruptions and glitches (technical glitches) and their impact on the investors' opportunity to trade constitutes major technology related risk. Thus, the following framework to deal with technical glitches occurring in the trading systems of Broker Dealers shall be complied with.

17.2. Definition of a Technical Glitch

A "Technical Glitch" shall mean any failure, interruption or malfunction, howsoever caused, affecting the Broker-Dealer's operational infrastructure. This includes, but not limited to: defects or errors in hardware, software, network connectivity, automated processes, and any electronic products, platforms, or services delivered by the Broker-Dealer.

The failure/interruption/malfunction may be experienced due to inadequate Infrastructure / systems, cyber-attacks / incidents, procedural errors and omissions, or process failures or otherwise, in their own systems or the one outsourced from any third parties, which may lead to either stoppage, slowing down or variance in the normal functions / operations / services of systems of the Broker Dealer for a contiguous period of five minutes or more.

17.3. Reporting Requirements

17.3.1. The Broker Dealers shall inform about the technical glitch to the Stock Exchanges immediately but not later than one hour from the time of occurrence of the glitch.

17.3.2. The Broker Dealers shall submit a Preliminary Incident Report to the Exchange within T+1 day of the incident (T being the date of the incident). The report shall include the date and time of the incident, the details of the incident, effect of the incident and the immediate action taken to rectify the problem.

17.3.3. The Broker Dealers shall submit a Root Cause Analysis (RCA) Report of the technical glitch to Stock Exchange, within fourteen days from the date of the incident.

17.3.4. RCA report submitted by the Broker Dealers shall, inter-alia, include time of incident, cause of the technical glitch (including root cause from vendor(s), if applicable), duration, chronology of events, impact analysis and details of corrective/ preventive measures taken (or to be taken), restoration of operations etc.

17.3.5. The Broker Dealers shall submit information stated in para 17.3.1, 17.3.2 and 17.3.3 above, to all The Stock Exchanges.

17.3.6. All technical glitches reported by Broker Dealers as well as independently monitored by The Stock Exchanges, shall be examined collectively by the Stock Exchanges along with the report/ RCA and appropriate action shall be taken.

17.4. Capacity Planning

17.4.1. Increasing number of investors may create additional burden on the trading system of the Broker Dealer and hence, adequate capacity planning is prerequisite for Broker Dealers to provide continuity of services to their clients. The Broker Dealers shall do capacity planning for entire trading infrastructure i.e. server capacities, network availability, and the serving capacity of trading applications.

17.4.2. The Broker Dealers shall monitor peak load in their trading applications, servers and network architecture. The Peak load shall be determined on the basis of highest peak load observed by the Broker Dealer during a calendar quarter. The installed capacity shall be at least one and half times (1.5x) of the observed peak load.

17.4.3. The Broker Dealers shall deploy adequate monitoring mechanisms within their networks and systems to get timely alerts on current utilization of capacity going beyond permissible limit of seventy percent of its installed capacity.

17.4.4. To ensure the continuity of services at the primary data center, Broker Dealers as may be specified from time to time by Stock Exchange shall strive to achieve full redundancy in their IT systems that are related to trading applications and trading related services.

17.4.5. The Stock Exchanges shall issue detailed guidelines with regard to frequency of capacity planning to review available capacity, peak load, and new capacity required to tackle future load on the system.

17.5. Software testing and change

17.5.1. Software applications are prone to updates/changes and hence, it is imperative for the Broker Dealers to ensure that all software changes that are taking place in their applications are rigorously tested before they are used in production systems. Software changes could impact the functioning of the software if adequate testing is not carried out. In view of this, The Broker Dealers shall adopt the following framework for carrying out software related changes / testing in their systems:

a. The Broker Dealers shall create test driven environments for all types of software developed by them or their vendors. Regression testing, security testing and unit testing shall be included in the software development, deployment and operations practices.

b. Specified Broker Dealers shall do their software testing in automated environments.

c. The Broker Dealers shall prepare a traceability matrix between functionalities and unit tests, while developing any software that is used in trading activities.

d. The Broker Dealers shall implement a change management process to avoid any risk arising due to unplanned and unauthorized changes for all its information security assets (hardware, software, network, etc.).

e. The Broker Dealers shall periodically update all their assets including Servers, OS, databases, middleware, network devices, firewalls, IDS /IPS desktops etc. with latest applicable versions and patches.

f. The Stock Exchanges shall issue detailed guidelines with regard to testing of software, testing in automated environments, traceability matrix, change management process and periodic updation of assets etc.

17.6. Monitoring mechanism

17.6.1. Proactively and independently monitoring technical glitches shall be one of the approaches in mitigating the impact of such glitches. In this context, the Stock Exchange shall build API based Logging and Monitoring Mechanism (LAMA) to be operated between the Stock Exchanges and specified Broker Dealers' trading systems. Under this mechanism, specified Broker Dealers shall monitor key systems & functional parameters to ensure that their trading systems function in a smooth manner. The Stock Exchanges shall, through the API gateway, independently monitor these key parameters to gauge the health of the trading systems of the specified Broker Dealers.

17.6.2. The Stock Exchanges shall identify the key parameters in consultation with the Broker Dealers. These key parameters shall be monitored by specified Broker Dealers and by the Stock Exchanges, on a real time or on a near real time basis.

17.6.3. The Stock Exchanges shall maintain a dedicated cell for monitoring the key parameters and the technical glitches occurring in the Broker Dealers' trading systems. The cell also shall intimate the specified Broker Dealer concerned immediately about the breach of the key parameters monitored under LAMA.

17.6.4. The Broker Dealers and Stock Exchanges shall preserve the logs of the key parameters for a period of thirty days in normal course. However, if a technical glitch takes place, the data related to the glitch, shall be maintained for a period of two years.

17.7. Business Continuity Planning (BCP) and Disaster Recovery Site (DRS)

17.7.1. The Broker Dealers as may be specified by Stock Exchanges (based on number of clients or any other criteria) from time to time, shall mandatorily establish business continuity/DR set up.

17.7.2. The Broker Dealers shall put in place a comprehensive BCP-DR policy document outlining standard operating procedures to be followed in the event of any disaster. A suitable framework shall be put in place to constantly monitor health and performance of critical systems in the normal course of

business. The BCP-DR policy document shall be periodically reviewed to minimize incidents affecting the business continuity.

17.7.3. The DRS shall preferably be set up in different seismic zones. In case, due to any reasons like operational constraints, such a geographic separation is not possible, then the Primary Data Centre (PDC) and DRS shall be separated from each other by a distance of at least two hundred and fifty (250) kilometers to ensure that both of them do not get affected by the same natural disaster. The DR site shall be made accessible from primary data center to ensure syncing of data across two sites.

17.7.4. It is clarified that operations carried out by the Broker Dealers and Clearing Members, from their respective DR sites located outside GIFT-IFSC and within India, shall be deemed to have been carried out at GIFT-IFSC.

17.7.5. Specified Broker Dealers shall conduct DR drills / live trading from DR site. DR drills / live trading shall include running all operations from DRS for at least 1 full trading day. Stock Exchanges in consultation with specified Broker Dealers shall decide the frequency of DR drill / live trading from DR site.

17.7.6. The Broker Dealers, shall constitute responsible teams for taking decisions about shifting of operations from primary site to DR site, putting adequate resources at DR site, and setting up mechanism to make DR site operational from primary data center etc.

17.7.7. Hardware, system software, application environment, network and security devices and associated application environments of DRS and PDC shall have one-to-one correspondence between them. Adequate resources shall be made available at all times to handle operations at PDC or DRS.

17.7.8. Stock Exchanges in consultation with the Broker Dealers shall decide upon Recovery Time Objective (RTO) i.e. the maximum time taken to restore operations from DRS after declaration of Disaster and, Recovery Point Objective (RPO) i.e. the maximum tolerable period for which data might be lost due to a major incident.

17.7.9. Replication architecture, bandwidth and load consideration between the DRS and PDC shall be within stipulated RTO and the whole system shall ensure high availability, right sizing, and no single point of failure. Any updates made at the PDC shall be reflected at DRS immediately.

17.7.10. Specified Broker Dealers shall obtain ISO certification as may be specified by Stock Exchanges from time to time in the area of IT and IT enabled infrastructure/processes of the Broker Dealers.

17.7.11. The System Auditor, while covering the BCP – DR as a part of mandated annual System Audit, shall check the preparedness of the Broker Dealer to shift its operations from PDC to DRS and also comment on documented results and observations on DR drills conducted by the Broker Dealers.

17.7.12. The Stock Exchanges shall define the term 'critical systems', 'disaster' and issue detailed guidelines with regard to review of BCP document, DR drill/live trading, operating DR site from PDC, timeline for obtaining ISO certification etc.

17.8. The Stock Exchanges shall put in place a structure of financial disincentives applicable to Broker Dealers for technical glitches occurring in their trading systems and non-compliance of the provisions made in this regard.

17.9. The Stock Exchanges shall disseminate on their websites the instances of Technical glitches occurred in the trading system of the Broker Dealers along with Root Cause Analysis (RCA) on such glitches.

CHAPTER V: INTERNAL POLICY ON OUTSOURCING OF ACTIVITIES

18 Internal Policy on Outsourcing

18.1 In terms of Code of Conduct provided under Schedule II of the CMI Regulations, the Broker Dealers or Clearing Members are required to have an internal policy for outsourcing of its activities from outside of IFSC.

18.2 The Broker Dealer or Clearing Member shall have an internal policy on outsourcing of activities prior to commencement of operations, and the Broker Dealer or Clearing Member shall ensure compliance with the policy at all times.

CHAPTER VI: COMPLAINT HANDLING AND GRIEVANCE REDRESSAL

19. Complaint Handling and Grievance Redressal

19.1. Regulation 18 of the CMI Regulations require that the Broker Dealers or Clearing Members in the IFSC shall take adequate steps for redressal of grievances of the investors in accordance with the requirements as may be specified by the Authority.

19.2. The Broker Dealer or Clearing Member shall comply with the applicable norms and requirements relating to handling of consumer complaints specified by the Authority by way of circular titled "Complaint Handling and Grievance Redressal by Regulated Entities in the IFSC" dated December 02, 2024 read with circular titled "Extension of timeline for implementation of the Circular titled "Complaint Handling and Grievance Redressal by Regulated Entities in the IFSC" dated December 02, 2024" issued on January 13, 2025.

CHAPTER VII: CHANGE IN CONTROL

20. Broker Dealers or Clearing Members operating in the IFSC in Branch Structure

20.1. In terms of regulation 23(1) of the CMI Regulations, the Broker Dealer or Clearing Member shall intimate the Stock Exchange / Clearing Corporation and IFSCA, within fifteen days of any direct or indirect change in control of the intermediary.

20.2. Broker Dealers or Clearing Members incorporated in the IFSC

20.2.1. In terms of regulation 23(2) of the CMI Regulations, the Broker Dealer or Clearing Member shall seek prior approval of the Authority, in case of any direct or indirect change in control of the entity.

20.2.2. Such an application for change in control shall be filed through respective Stock Exchange / Clearing Corporation.

20.3. Information to be submitted while seeking prior approval or submitting intimation regarding change in control

20.3.1. The Broker Dealers or Clearing Members shall provide the following information while submitting application for seeking prior approval regarding change in control:

a. Details of new shareholders / entities exercising control over the Broker Dealer or Clearing Member along with number of shares, per cent. of shares etc.;

b. A declaration that the new shareholders/ entities exercising control are “fit and proper” in accordance with the criteria specified under regulation 8 of the CMI Regulations;

c. Details of any material regulatory action taken or pending against the Broker Dealer or Clearing Member or any of its controlling shareholder or director by any financial sector regulator in the last three years.

d. A confirmation that all fees due to IFSCA as per the IFSCA Fee Circular has been paid

e. Number of investor complaints pending, if any, at the time of filing application/ intimation.

f. Details of ongoing material litigations, if any.

g. Copies of board resolution and shareholder resolution, as applicable, relating to change in control.

h. Any other information as may be specified by the Stock Exchange / Clearing Corporation / IFSCA

CHAPTER VIII: PERIODIC REPORTING TO THE IFSCA

21. Quarterly Reporting

21.1. The Broker Dealer or Clearing Member shall submit reports to the IFSCA on a quarterly basis in accordance with the requirements specified under the circular titled "Reporting Norms for Capital Market Intermediaries" dated February 08, 2024 (as amended from time to time).

21.2. The Broker Dealer or Clearing Member shall furnish such information, documents, or records as may be specified by IFSCA from time to time.

22. Annual Compliance Audit

22.1. In terms of regulation 25 of the CMI Regulations, the Broker Dealer or Clearing Member shall have an annual audit conducted in respect of compliance with the CMI Regulations by a member of the Institute of Chartered Accountants of India or a member of the Institute of Company Secretaries of India or a member of the Institute of Cost Accountants of India or any person authorised to conduct audit in a Foreign Jurisdiction.

22.2. A copy of such compliance audit report for a financial year shall be furnished to IFSCA by the 30th of September of such year.

22.3. It is also clarified that Broker Dealers shall also submit a copy of such audit report to the Stock Exchanges. The Stock Exchanges shall be required to submit a summary of audit findings along with its recommendations to IFSCA by 30th of November of every year.

22.4. The Broker Dealer or Clearing Member shall have additional audits and submit such reports as may be specified by IFSCA from time to time.

CHAPTER IX: SURRENDER OF REGISTRATION

23. Surrender of Registration

23.1. In terms of regulation 14 of the CMI Regulations, a Broker Dealer or Clearing Member may file an application with the Authority for surrender of its registration.

23.2. Such an application for surrender of registration shall be filed through the respective Stock Exchange / Clearing Corporation.

23.3. The Broker Dealer or Clearing Member shall provide the following information while submitting application for surrender of registration:

23.3.1. Details of registration;
23.3.2. Original Certificate of Registration (if issued in physical form);
23.3.3. List of all activities that are being carried out by the entity;
23.3.4. Details of registration in any other capacity with IFSCA;
23.3.5. List of controlling shareholders and directors;
23.3.6. Details of any material regulatory action taken or pending against the Broker Dealer or Clearing Member or any of its controlling shareholder or director by any financial sector regulator in the last three years;
23.3.7. Details of ongoing material litigations, if any;
23.3.8. Copies of board resolution and shareholder resolution, as applicable, relating to surrender of registration;
23.3.9. Reasons for surrender of registration; and
23.3.10. Undertaking as under:

Whether any disciplinary proceeding is pending against the Applicant	
Whether any investigation/adjudication/ enquiry by IFSCA is pending against the applicant or its controlling shareholders and directors	
Whether as on date of application all fees have been paid and also mention the date of next due date of payment of fee	
Whether any arrangements made by the applicant for maintenance and preservation of records and other documents required to be maintained under the relevant regulations /guidelines of IFSCA	
Whether any arrangements made to transfer its activities to another intermediary holding a valid certificate of registration to carry on such activity	

Whether there are any investor complaints pending against the applicant as on the date of application.	

24. Refund of security deposit to Broker Dealers on surrender of membership

24.1. On approval of application for surrender of Broker Dealer's registration by IFSCA, the Stock Exchange shall release Security Deposit of the Broker Dealer (engaged in trading on behalf of clients) after twelve months from the date of approval of surrender application by IFSCA.

24.2. On approval of application for surrender of Broker Dealer's registration by IFSCA, the Exchange shall release Security Deposit of the Broker Dealer (engaged only in proprietary trading for the last three years prior to the date of application of surrender) after six months from the date of approval of surrender application by IFSCA.

Annexure - 1

1. Terms of Reference (ToR) for Type I Broker The system auditor shall at the minimum cover the following areas:

1.1. System controls and capabilities

1.1.1. 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.

1.1.2. Order Status/ Capture – Whether the system has capability to generate / capture order id, time stamping, order type, scrip details, action, quantity, price and validity etc.

1.1.3. Rejection of orders – Whether system has capability to reject orders which do not go through order level validation at the end of the Broker Dealer and at the servers of respective Stock Exchanges.

1.1.4. 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 email; facility of viewing trade log.

1.1.5. 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.

1.2. Risk Management System (RMS)

1.2.1. 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.

1.2.2. 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 permitted 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.

1.2.3. 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.

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

1.2.5. 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.

1.2.6. 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.

1.3. Password Security

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

1.3.2. 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.

1.3.3. 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.

1.4. Session Management

1.4.1. 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.

1.4.2. 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.

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

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

1.5. Network Integrity

1.5.1. Seamless connectivity – Whether Broker Dealer has ensured that a backup network link is available in case of primary link failure with the exchange.

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

1.5.3. Firewall Configuration – Whether appropriate firewall is present between Broker Dealer's trading setup and various communication links to the exchange. Whether the firewall is appropriately configured to ensure maximum security.

1.6. Access Controls

1.6.1. Access to server rooms – Whether adequate controls are in place for access to server rooms and proper audit trails are maintained for the same.

1.6.2. 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

1.7. Backup and Recovery

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

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

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

1.8. BCP/DR (Only applicable for Broker Dealers having BCP / DR site)

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

1.8.2. Alternate channel of communication – Whether the Broker Dealer 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).

1.8.3. 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.

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

1.8.5. Segregation of Data and Processing facilities – The system auditor should check and comment on the segregation of data and processing facilities at the Broker Dealer in case the Broker Dealer is also running other business.

1.9. Back office data

1.9.1. 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.

1.9.2. 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.

1.10. 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))

1.10.1. 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.

1.10.2. 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.

1.10.3. 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.

1.10.4. 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.

1.11. 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 - 2

ToR for Type II Broker

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

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

1.1.1. 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.

1.1.2. Order Status/ Capture – Whether the system has capability to generate / capture order id, time stamping, order type, scrip details, action, quantity, price and validity, etc.

1.1.3. 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.

1.1.4. Communication of Trade Confirmation / Order Status – Whether the system has capability to timely communicate to Client regarding the Acceptance/ Rejection of an Order / Trade via various media including e-mail; facility of viewing trade log.

1.1.5. 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.

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

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

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

1.2.2. Fault reporting / tracking mechanism and process for resolution. Testing of new releases / patches / modified software / bug fixes.

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

1.2.4. Development / Test / Production environment segregation.

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

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

1.2.7. 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.

1.3. Risk Management System (RMS)

1.3.1. 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.

1.3.2. 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 permitted 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.

1.3.3. 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.

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

1.3.5. 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.

1.3.6. 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.

1.4. Password Security

1.4.1. 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.

1.4.2. 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.

1.4.3. 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.

1.5. Session Management

1.5.1. 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.

1.5.2. 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.

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

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

1.6. Database Security

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

1.6.2. 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.

1.7. Network Integrity

1.7.1. Seamless connectivity – Whether the Broker Dealer has ensured that a backup network link is available in case of primary link failure with the exchange.

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

1.7.3. Firewall Configuration – Whether appropriate firewall is present between Broker Dealer's trading setup and various communication links to the exchange. Whether the firewall is appropriately configured to ensure maximum security.

1.8. Access Controls

1.8.1. Access to server rooms – Whether adequate controls are in place for access to server rooms and proper audit trails are maintained for the same.

1.8.2. 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.

1.9. Backup and Recovery

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

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

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

1.10. BCP/DR (Only applicable for Broker Dealers having BCP / DR site)

1.10.1. BCP / DR Policy – Whether the Broker Dealer has a well-documented BCP/ DR policy and plan. The system auditor should comment on the documented incident response procedures.

1.10.2. Alternate channel of communication – Whether the Broker Dealer 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).

1.10.3. 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.

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

1.11. Segregation of Data and Processing facilities – The system auditor should check and comment on the segregation of data and processing facilities at the Broker Dealer in case the Broker Dealer is also running other business.

1.12. Back office data

1.12.1. 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.

1.12.2. 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.

1.13. User Management

1.13.1. User Management Policy – The system auditor should check whether the Broker Dealer has a well-documented policy that provides for user management and the user management policy explicitly defines user, database and application Access Matrix.

1.13.2. 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.

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

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

1.14. 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))

1.14.1. 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.

1.14.2. 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.

1.14.3. 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. 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.

1.15. 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.

1.16. Software Testing Procedures - The system auditor should check whether the Broker Dealer has complied with the guidelines and

instructions of IFSCA / Stock Exchanges with regard to testing of software and new patches, including the following:

1.16.1. Test Procedure Review – The system auditor should evaluate whether the procedures for system and software testing were proper and adequate. 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.

1.16.2. 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 IFSCA.

Annexure - 3

ToR for Type III Broker

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

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

1.1.2. 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.

1.1.3. Order Status/ Capture – Whether the system has capability to generate / capture order id, time stamping, order type, scrip details, action, quantity, price and validity etc.

1.1.4. 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.

1.1.5. Communication of Trade Confirmation / Order Status – Whether the system has capability to timely communicate to client regarding the Acceptance/ Rejection of an Order / Trade via various media including e-mail; facility of viewing trade log.

1.1.6. 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.

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

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

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

1.2.2. Fault reporting / tracking mechanism and process for resolution.

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

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

1.2.5. Development / Test / Production environment segregation.

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

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

1.2.8. 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.

1.3. Risk Management System (RMS)

1.3.1. 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.

1.3.2. 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 permitted 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.

1.3.3. 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.

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

1.3.5. 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.

1.3.6. 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.

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

1.4.1. 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.

1.4.2. 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.

1.4.3. 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.

1.4.4. 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.

1.4.5. Check for preventing loop or runaway situations – The system auditor should check whether the Broker Dealers have real time monitoring systems to identify and shutdown/stop the algorithms which have not behaved as expected.

1.4.6. 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.

1.5. Audit Trail – The system auditor should check the following areas in audit trail:

1.5.1. Whether the audit trails can be established using unique identification for all algorithmic orders and comment on the same.

1.5.2. Whether the broker maintains logs of all trading activities.

1.5.3. Whether the records of control parameters, orders, traders and data emanating from trades executed through algorithmic trading are preserved/ maintained by the Broker Dealer.

1.5.4. 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.

1.5.5. Whether the system captures the IP address from where the algo orders are originating.

1.6. Systems and Procedures – The system auditor should check and comment on the procedures, systems and technical capabilities of Broker Dealer 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.

1.6.1. Reporting to Stock Exchanges – The system auditor should check whether the Broker Dealer 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 Broker Dealer to inform the Stock Exchanges regarding such incidents.

1.7. Password Security

1.7.1. Organization Access Policy – The system auditor should verify whether the Broker Dealer 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.

1.7.2. 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.

1.7.3. Password Best Practices – Whether there is a system 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.

1.8. Session Management

1.8.1. 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.

1.8.2. 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.

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

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

1.9. Database Security

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

1.9.2. 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.

1.10. Network Integrity

1.10.1. Seamless connectivity – Whether the Broker Dealer has ensured that a backup network link is available in case of primary link failure with the exchange.

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

1.10.3. Firewall Configuration – Whether appropriate firewall is present between the Broker Dealer's trading setup and various communication links to the exchange. Whether the firewall should be appropriately configured to ensure maximum security.

1.11. Access Controls

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

1.11.2. 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.

1.12. Backup and Recovery

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

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

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

1.13. BCP/DR (Only applicable for Broker Dealers having BCP / DR site)

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

1.13.2. Alternate channel of communication – Whether the Broker Dealer 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).

1.13.3. 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.

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

1.13.5. Segregation of Data and Processing facilities – The system auditor should check and comment on the segregation of data and processing facilities at the Broker Dealer in case the Broker Dealer is also running other business.

1.14. Back office data

1.14.1. 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.

1.14.2. 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.

1.15. User Management

1.15.1. User Management Policy – The system auditor should verify whether the Broker Dealer has a well documented policy that provides for user management and the user management policy explicitly defines user, database and application access matrix.

1.15.2. 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.

1.15.3. 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.

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

1.16. 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))

1.16.1. 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.

1.16.2. 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.

1.16.3. 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.

1.16.4. 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.

1.17. 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.

1.17.1. Software Testing Procedures - The system auditor shall audit whether the Broker Dealer has complied with the guidelines and instructions of IFSCA / Stock Exchanges with regard to testing of software and new patches including the following

1.17.2. 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.

1.17.3. 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.

1.17.4. 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 and various IFSCA Circulars.

Annexure - 4

For Preliminary Audit

Audit Date	Observation	Description of Finding	Department	Status/ Nature of Findings	Risk Ratings of Findings	Audited TOR Clause	Audited By	Root Cause Analysis	Impact Analysis	Suggested Correction	Deadline for 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

For Follow on / Follow up System Audit

Preliminary Audit Date	Sr. No.	Preliminary Observation Number	Preliminary Status	Preliminary Current Action	Current Finding	Current Status	Revised Correction	Deadline for the revised correction	Verified by	Closing date

Description of relevant Table heads

9. Preliminary Status – The original finding as per the preliminary System Audit Report.

10. Preliminary Corrective Action – The original corrective action as prescribed in the preliminary System Audit report.

11. Current Finding – The current finding w.r.t. the issue.

12. Current Status – Current status of the issue viz Compliant, Non-Compliant, Work In Progress (WIP).

13. Revised Corrective Action – The revised corrective action prescribed w.r.t. the Non-Compliant / WIP issues.

Annexure - 5

Regulatory Framework for Market Access to IFSC based Stock Exchanges through Authorized Persons

1. Who is an "Authorized Person"?

Any person - individual, partnership firm, LLP or body corporate – who is appointed as such by a Broker Dealer and who provides access to the trading platform of a Stock Exchange as an agent of the Broker Dealer.

2. Appointment of Authorized Person

A Broker Dealer may appoint one or more Authorized Person(s) after obtaining specific prior approval from the stock exchange concerned for each such person.

3. Procedure for Appointment

a) The Broker Dealer shall select a person in compliance with the criteria laid down by the Exchange and this framework for appointment as an Authorized Person and forward the application of the person to stock exchange for approval.

b) On receipt of the aforesaid application, the stock exchange

i. shall accord approval on satisfying itself that the person is eligible for appointment as Authorized Person,
or
ii. shall refuse approval on satisfying itself that the person is not eligible for appointment as Authorized Person

4. Eligibility Criteria

I. An individual is eligible to be appointed as Authorized Person if he:

a) is a citizen of India or a citizen of any of the Financial Action Task Force (FATF) compliant jurisdictions;
b) is not less than 18 years of age;
c) has not been convicted of any economic/financial offence in his home jurisdiction or overseas;
d) has a good reputation and character;
e) is a graduate from a recognized institution in the jurisdiction of his citizenship; and
f) the approved users and / or sales personnel of the Authorized Person shall have the necessary certifications, prescribed by the stock exchanges, at all points of time

II. A partnership firm, LLP or a body corporate is eligible to be appointed as an Authorized Person if;

a) it is incorporated in the IFSC or in any of the FATF compliant jurisdictions or which is governed by an FATF style regional body
b) if all the partners or directors, as the case may be, comply with the requirements contained in clause I above
c) the object clause of the partnership deed or of the Memorandum of Association contains a clause permitting the person to deal in securities business

III. The person shall have the necessary infrastructure like adequate office space, equipment and manpower to effectively discharge the activities on behalf of the Broker Dealer.

5. Conditions of Appointment

The following are the conditions of appointment of an Authorized Person:

a) The Broker Dealer shall be responsible for all acts of omission and commission of the Authorized Person
b) All acts of omission and commission of the Authorized Person shall be deemed to be those of the Broker Dealer
c) The Authorized Person shall not receive or pay any money or securities in its own name or account. All receipts and payments of securities and funds shall be in the name or account of the Broker Dealer
d) The Authorized Person shall receive his remuneration - fees, charges, commission, salary, etc. - for his services only from the Broker Dealer and he shall not charge any amount from the clients
e) A person shall not be appointed as an Authorized Person by more than one Broker Dealer on the same stock exchange
f) A partner or director of an Authorized Person shall not be appointed as an Authorized Person on the same stock exchange
g) The Broker Dealer and Authorized Person shall enter into written agreement(s) in the form(s) specified by the stock exchange. The agreement shall inter-alia cover the scope of the activities, responsibilities, confidentiality of information, commission sharing, termination clause, etc.

6. Withdrawal of Approval

The approval given to an Authorized Person shall be withdrawn by the stock exchange:

a) on receipt of a request to that effect from the concerned Broker Dealer or the Authorized Person, subject to compliance with the requirements prescribed by the stock exchange,
or
b) on being satisfied that the continuation of the Authorized Person is detrimental to the interest of investors or the securities market
or
c) the Authorized Person at a subsequent date fails to fulfil the eligibility criteria specified at clause 4.

7. Obligations of a Broker Dealer

a) The Broker Dealer shall be responsible for all acts of omission and commission of his Authorized Person(s) and/or their employees, including liabilities arising therefrom

b) If any trading terminal is provided by the Broker Dealer to an Authorized Person, the place where such trading terminal is located shall be treated as the branch office of the Broker Dealer

c) The Broker Dealer shall display at each branch office additional information such as particulars of the Authorized Person in charge of that branch, time lines for dealing through the Authorized Person, etc., as may be specified by the stock exchange

d) The Broker Dealer shall notify changes, if any, in the Authorized Person to all registered clients of that branch at least thirty days before the change

e) The Broker Dealer shall conduct periodic inspection of branches assigned to the Authorized Persons and the records of the operations carried out by them

f) The client shall be registered with the Broker Dealer only. The funds and securities of the clients shall be settled directly between the Broker Dealer and the client and all documents like contract notes, statement of funds and securities shall be issued to the client by the Broker Dealer. The Authorized Person may provide administrative assistance in procurement of documents and settlement, but shall not issue any document to the client in his own name. No fund/securities of the clients shall be credited to the accounts of the Authorized Person

g) On noticing any irregularities in the operations of the Authorized Person, the Broker Dealer shall:

i. seek withdrawal of approval of the Authorized Person,
ii. withhold all moneys due to Authorized Person till resolution of client complaint,
iii. alert clients / potential investors in the location where such an Authorized Person operates,
iv. file a complaint with the police and take all measures required to protect the interest of the investors and the market

8. Obligations of the Stock Exchange

a) The Stock Exchanges shall maintain a database of all the Authorized Persons which shall include the following:

i. Tax Id of home jurisdiction of individual Authorized Person and in case of a partnership, LLP or body corporate, the Tax id of the home jurisdiction of all the partners or directors and Legal Entity Identifier (LEI) number of the entity as the case may be
ii. Details of the Broker Dealer with whom the Authorized Person is registered
iii. Locations of branch assigned to the Authorized Person(s)
iv. Number of terminals and their details, given to each Authorized Person.
v. Withdrawal of approval of the Authorized Person
vi. Change in status or constitution of the Authorized Person
vii. Disciplinary action taken by the Exchange against the Authorized Person

The data pertaining to points 8(a)(ii) to 8(a)(vii) above shall be made available on websites of the stock exchanges.

b) While conducting the inspection of the Broker Dealer, the stock exchange shall also conduct inspection of branches (where the terminals of the Authorized Persons are located) and records of the operations carried out by them

c) The dispute between a client and an Authorized Person shall be treated as a dispute between the client and the Broker Dealer. The Stock Exchanges shall put in place the appropriate dispute resolution/ redressal mechanisms accordingly

d) In case of withdrawal of approval of Authorized Person due to disciplinary action, the stock exchange shall disseminate the names of such Authorized Persons on its website citing the reason for cancellation