MASTER CIRCULAR

IFSCA/CMD/MIIT/MCBDCM/2026 **May 12, 2026**

To,

All Stock Exchanges in the International Financial Services Centre (IFSC);
All Clearing Corporations in the IFSC;
All Broker Dealers in the IFSC;
All Clearing Members in the IFSC.

Madam/Sir,

Subject: Master Circular for Broker Dealers and Clearing Members

1. Reference may be drawn to the International Financial Services Centres Authority (Capital Market Intermediaries) Regulations, 2021, and the circulars issued thereunder.

2. Subsequently, the International Financial Services Centres Authority ('Authority' / 'IFSCA') issued the International Financial Services Centres Authority (Capital Market Intermediaries) Regulations, 2025 ('CMI Regulations') which repealed the International Financial Services Centres Authority (Capital Market Intermediaries) Regulations, 2021, while specifying a unified framework for the regulation and supervision of Capital Market Intermediaries, which, *inter-alia*, includes Broker Dealers and Clearing Members.

3. The Authority, being satisfied that it is necessary and expedient for ease of doing business and for overall development of the IFSC ecosystem, hereby consolidates all the circulars pertaining to Broker Dealers and Clearing Members and issues this Master Circular.

4. (i) On and from the date of commencement of this Master Circular, the following circulars issued by the Authority shall stand superseded:

Sr. No.	Date	Circular No.	Subject
1	October 14, 2020	F. No. 68/IFSCA/MRD-AP/2020-21	Market Access through Authorized Persons

Sr. No.	Date	Circular No.	Subject
2	April 13, 2021	F. No. 286/IFSCA/Policy Matters (CMD-DMIIT)/2021	Fee structure for Market Infrastructure Institutions (MIIs) and Participants
3	September 15, 2021	F. No. 224/IFSCA/CMD-DMIIT/CUST/2021/2	Clearing Membership for non-bank Custodians
4	April 29, 2022	IFSCA/CMD-DMIIT/AP/2022-23/1	Market Access through Authorized Person
5	June 28, 2022	IFSCA/CMD-DMIIT/BD/2022-23/1	Refund of security deposit to Broker Dealers on surrender of membership
6	May 09, 2023	IFSCA/CMD-DMIIT/BCP-DR/2023-24/001	Status of operations at Disaster Recovery (DR) Site of the Broker Dealers and Clearing Members registered with IFSCA
7	March 14, 2024	IFSCA/CMD-DMIIT/SOF/2023-24/001	Ease of doing business: Settlement of Client's Funds lying with Broker Dealer

(ii) On and from the date of commencement of this Master Circular, all circulars and guidelines issued by the Securities and Exchange Board of India ("SEBI") prior to October 01, 2020, in respect of a Broker Dealer/Clearing Member registered with the Authority, shall stand superseded.

(iii) This Master Circular shall be applicable to Broker Dealers for their activities on the recognised stock exchanges in the IFSC and is not applicable for the activities related to global access by the Broker Dealers. Global access by the Broker Dealers shall be governed through the separate circulars/regulatory framework issued by the Authority for global access by Broker Dealers.

(iv) Notwithstanding the supersession specified in (i) and (ii) above,

a) anything done or any action taken or purported to have been done or taken under the superseded circulars, prior to such supersession, shall be deemed to have been done or taken under the corresponding provisions of this Master Circular; and

b) any application made to the Authority under any of the superseded circular(s) prior to such supersession shall be deemed to have been made under the corresponding provisions of this Master Circular;

5. This Master Circular is being issued in exercise of powers conferred by Sections 12 and 13 of the International Financial Services Centres Authority Act, 2019, read with regulation 45 of the CMI Regulations and regulation 72 of the IFSCA (Market Infrastructure Institutions) Regulations, 2021, and shall come into force from the date of its issuance.

A copy of this circular is available on the website of the International Financial Services Centres Authority at www.ifsca.gov.in.

Yours faithfully

Praveen Kamat
General Manager
Division of Market Infrastructure Institutions & Technology
Capital Markets Department
Email: praveen.kamat@ifsca.gov.in
Tel: +91-079-61809820

Table of Contents

CHAPTER – I: PROCESS OF REGISTRATION

1. Application for Registration

1.1. The International Financial Services Centres Authority (IFSCA/the Authority) 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. The link for accessing the SWITS platform is https://swit.ifsca.gov.in.

1.2. 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.

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

1.4. An entity desirous of seeking registration as a Broker Dealer/Clearing Member with the Authority shall submit/file its applications exclusively through the SWIT System for seeking:

1.4.1. Registration as Broker Dealer/Clearing Member under the provisions of the CMI Regulations;
1.4.2. Approval from SEZ Authorities and GST registration; and
1.4.3. NoC/requisite approval from appropriate regulators (if any).

1.5. In this regard, for more details, Circular No. IFSCA-ITIn0WEB/1/2023-IT Infrastructure and Fintech- Part (1), titled "*Single Window IT System inter-alia for registration and approval from IFSCA, SEZ authorities, GSTN, RBI, SEBI and IRDAI*", dated September 30, 2024, issued by the Authority, may be referred to.

1.6. The Authority has also permitted the entities to apply for Unified Registration (Master Key), under the CMI Regulations, in accordance with its Circular No. IFSCA-PLNP/80/2024-Capital Markets, titled "*Unified Registration for multiple Capital Market Activities under the IFSCA (Capital Market Intermediaries) Regulations, 2025 (Master Key)*", dated February 13, 2026.

2. Payment of Fees

2.1. An applicant seeking registration as a Broker Dealer/Clearing Member under the CMI Regulations shall pay the application fee, as specified in Schedule-I of Circular No. IFSCA-DTFA/1/2026, titled "*Fee structure for the entities undertaking or intending to undertake permissible activities in IFSC or persons seeking guidance under the Informal Guidance Scheme*", ('IFSCA Fee Circular') dated March 02, 2026 at the time of making the 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 in-principle approval, the applicant shall, within 15 days of such intimation, pay the applicable registration fees as specified in Schedule-I of the IFSCA Fee Circular.

2.3. Where the Authority subsequently decides not to grant registration to the applicant to whom a provisional/ in-principle approval was granted, the fees paid by the applicant seeking registration shall not be refunded.

2.4. In cases where the applicant fails to pay the requisite registration fees within the specified time, it shall be assumed that the applicant does not wish to obtain registration, and the Authority may at its discretion discontinue the process and close the application:

Provided that where an applicant wishes to seek the registration after such closure, it shall be required to make a fresh application.

2.5. An application once rejected shall be considered *void ab initio*. While such rejection does not preclude the entity from submitting a new application, the subsequent filing shall be treated independently.

2.6. The fees as specified in the Schedule-I of the IFSCA Fee Circular shall be paid to the following account of the Authority in US Dollars:

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

2.7. An applicant from India (other than an entity already set up in IFSC) desirous of getting a registration from the Authority shall have the option to pay only the application fees and registration fees, 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

2.8. For the entities remitting fees in INR, the FBIL reference rate for USD-INR, of the date on which the remittance is being made, shall be applicable. The URL to access the FBIL website is as follows:
https://www.fbil.org.in/#/home

2.9. 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.

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

2.11. 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 Key Managerial Personnels (KMPs). In case the payment has been made from the account of the KMP(s), the same shall be intimated to the Authority at the time of submission of documentary evidence. However, in case

of initial payment of application and registration fee, such amount can be paid either by the parent or the promoter of the applicant.

2.12. A Broker Dealer/Clearing Member registered 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/Clearing Member shall be perpetual, unless it is suspended or cancelled by the Authority.

3.2. The Broker Dealer/Clearing Member shall always ensure that it holds valid and subsisting:

a) Certificate of Registration issued by the Authority under the CMI Regulations; and
b) 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 (which has validity of 1 year, if business has not commenced, or 5 years, after commencement of business, as the case may be) 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/Clearing Member shall ensure compliance with Circular No. IFSCA-LPRA/9/2024-Legal and Regulatory Affairs, titled "*Direction for all Regulated Entities*", dated April 03, 2025, issued by the Authority.

CHAPTER – II: ELIGIBILITY CRITERIA AND PERMISSIBLE ACTIVITIES

4. Eligibility Criteria

4.1. A Broker Dealer/Clearing Member shall be required to fulfil the eligibility criteria as prescribed under the Securities Contracts (Regulation) Act, 1956 (SCRA) and the Securities Contracts (Regulation) Rules, 1957 (SCRR).

4.2. The Broker Dealer/Clearing Member shall be set up in the IFSC in the form of a company, Limited Liability Partnership (LLP), body corporate, or a branch thereof.

4.3. Registration granted to the Broker Dealer/Clearing Member is strictly contingent upon the continuous adherence to the requirements mandated under the CMI Regulations.

4.4. An entity which is registered with SEBI as Stock Broker and is desirous of undertaking the securities market related activities in the IFSC is required to comply with the provisions of the Circular No. SEBI/HO/MIRSD/MIRSD-PoD/P/CIR/2025/61, titled "*Measures for Ease of Doing Business – Facilitation to SEBI registered Stock Brokers to undertake securities market related activities in Gujarat International Finance Tech-city – International Financial Services Centre (GIFT-IFSC) under a Separate Business Unit (SBU)*", dated May 02, 2025, issued by SEBI.

4.5. A non-bank custodian operating under a branch structure within the IFSC is authorized to act as a Clearing Member exclusively for its own custodial clients. Such entities are strictly prohibited from clearing or settling trades for third-party market participants or proprietary accounts.

5. Permissible Activities

5.1 A Broker Dealer/Clearing Member shall not be permitted to carry out the activities which are prohibited (not permitted) under the SCRA and SCRR. Rule 8 of the SCRR may please be referred to.

6. Net Worth

6.1. A Broker Dealer/Clearing Member shall comply with the net worth requirements as specified by the Stock Exchange/Clearing Corporation.

6.2. In cases where the Broker Dealer/Clearing Member is set up in the form of branch, the minimum net worth requirement may be maintained at the parent level in home jurisdiction where its parent entity is incorporated:

Provided that the minimum net worth maintained at the parent level shall be earmarked for its branch in IFSC.

6.3. Net worth for a Broker Dealer/Clearing Member shall mean the aggregate value of its liquid assets.

Explanation: Liquid assets shall mean cash and bank balance, fixed deposits, Government Securities and other instruments as may be specified by the Authority.

6.4. For the purpose of computation of liquid net worth, the Broker Dealer/Clearing Member may refer to the Circular No. IFSCA-PLNP/80/2024-Capital Markets, titled "*Computation of liquid net worth under IFSCA (Capital Market Intermediaries) Regulations, 2025 – Clarifications*", dated December 30, 2025, issued by the Authority.

CHAPTER – III: GOVERNANCE

7. Principal Officer

7.1. The Broker Dealer/Clearing Member shall have a Principal Officer who is based out of the IFSC and complies with the qualification and educational requirements as specified in the CMI Regulations.

7.2. The Principal Officer shall be responsible for overall activities of a Broker Dealer/Clearing Member in the IFSC.

7.3. Where a Broker Dealer/Clearing Member holds multiple registrations under the CMI Regulations, the Principal Officer shall be appointed/designated for each such registration separately:

Provided that where a Broker Dealer/Clearing Member is also registered with the Authority as depository participant, investment adviser, research entity, custodian, or registered distributor, it may have the same person as Principal Officer:

Provided further that a Broker Dealer/Clearing Member also having registration as Distributor shall have a separate official as a vertical head for its distribution business activities.

8. Compliance Officer

8.1. A Broker Dealer/Clearing Member shall have a Compliance Officer who is based out of the IFSC and complies with the qualification and educational requirements as specified in the CMI Regulations.

8.2. Where a Broker Dealer/Clearing Member holds multiple registrations under the CMI Regulations, it may have the same person as compliance officer for ensuring compliances with all the applicable regulatory and legal requirements for its activities as capital market intermediary in the IFSC.

9. Code of Conduct

9.1 A Broker Dealer/Clearing Member shall establish a Code of Conduct based on Schedule II of the CMI Regulations.

CHAPTER – IV: SUPERVISION & OVERSIGHT

10. **Oversight of Broker Dealers or Clearing Members**

10.1. Inspection of members by recognised stock exchanges/recognised clearing corporations (Stock Exchanges/Clearing Corporations)

10.1.1. To safeguard market stability, the Stock Exchange/Clearing Corporation shall formulate a policy for periodic and ad-hoc inspection of their members. The policy shall, inter-alia, cover various kinds of risks posed to the investors and the market at large on account of the activities/business conduct of their members.

10.1.2. The Stock Exchange/Clearing Corporation shall conduct inspection in accordance with its established policy. For entities holding multiple memberships across market infrastructure institutions (MIIs), a mandatory information sharing protocol shall be established between all relevant MIIs. Material findings and adverse inspection outcomes shall be communicated across these channels to ensure synchronized and holistic supervision. Any cases of repetitive and / or serious violations shall be brought to the notice of IFSCA.

10.1.3. The inspection shall, *inter-alia*, be conducted to check:

10.1.3.1. Compliance with the requirements of –

a) the relevant provisions of the IFSCA Act, 2019, the Securities and Exchange Board of India (SEBI) Act, 1992, SCRA and the Rules and Regulations made there under;
b) the Rules and Regulations of the Stock Exchange/Clearing Corporation; and
c) the circulars issued by IFSCA and Stock Exchanges/Clearing Corporations from time to time.

10.1.3.2. 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.

10.1.3.3. The Stock Exchange/Clearing Corporation shall ensure that all remedial, penal, and disciplinary action, as the case may be, arising from the findings of the inspection, is/are initiated within six months of the conclusion of the inspection. Any deviation from this timeline shall be justified to the Authority in writing.

10.1.3.4. The Clearing Corporation shall maintain primary oversight of, and conduct inspection in respect of, all clearing and settlement activities executed by a Clearing Member. The Stock Exchange shall have primary oversight of, and conduct inspection in respect of, the operations and business conduct of its Broker Dealers. To ensure comprehensive risk assessment and minimize regulatory overlap, the Stock Exchange and Clearing Corporation are encouraged to conduct joint inspections of dual-registered entities.

10.1.4. A Stock Exchange and Clearing Corporation may also conduct joint inspection with other Stock Exchanges and Clearing Corporations.

10.1.4.1. The Stock Exchanges and Clearing Corporations shall maintain a continuous risk-assessment framework to monitor the evolving profiles of their members and review/revise the policy of annual inspection, as and when required, to ensure that supervision remains proportionate to the systemic, operational and conduct risks identified within the market.

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

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

10.3. Standard Operating Procedure for Stock Exchanges / Clearing Corporations in response to event-based discrepancies :

10.3.1. The Stock Exchange/Clearing Corporation shall establish a robust Event Based Surveillance (EBS) mechanism, leveraging market intelligence and dynamic data to identify high-risk behaviours. An illustrative list of criteria for EBS is given below:

a. Failure to furnish net worth certificate within specified timelines.

b. Non-submission of 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 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.

10.4. With respect to net worth criteria, it is clarified that a Broker Dealer/Clearing Member failing to maintain the requisite net worth at any time shall not undertake any existing or new business activity in the IFSC till the time the net worth is restored. In this regard, Circular No. IFSCA-DSI/4/2024-Capital Markets, titled "*Maintenance of Net Worth by Capital Market Intermediaries*", dated September 05, 2024, issued by the Authority, may please be referred to.

11. Running Account Settlement

11.1. Unless otherwise directed by the Authority, the settlement of funds shall be governed by the agreement entered into by the Broker Dealer and the client or the consent letter issued by the client in favour of the Broker Dealer. To ensure market-wide uniformity and investor protection, the Stock Exchanges shall prescribe a standardized format for such agreements, which all Broker Dealers shall adopt. Such documentation shall be duly executed at the time of client onboarding.

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

12. **System Audit of Broker Dealers**

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

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

12.3. The Stock Exchanges are advised to keep track of findings of system audits of all Broker Dealers and ensure that all major audit findings, specifically in critical areas, are rectified/complied within timelines specified by the Stock Exchanges failing which follow up inspection of such Broker Dealers may be taken up for necessary corrective steps/actions thereafter, if any.

12.4. The Stock Exchange shall report all major non-compliances / observations of system auditors, Broker Dealer wise, on an annual basis, to the Authority, within 4 months from the end of the audit period.

12.4.1. Audit Process

12.4.1.1. The system audit of Broker Dealers shall be conducted on an annual basis.

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

a. Type I:
Broker Dealers who trade through exchange provided terminals such as National Exchange for Automated Trading (NEAT), BSE's Online Trading System (BOLT) etc. (ToR attached as **Annexure-1**);

b. 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**)

c. 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**)

12.4.2. 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. Such an auditor / audit firm can be reappointed after a cooling off period of 2 years.

12.4.3. 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.

12.4.4. 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.

12.4.5. 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.

12.4.6. 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.

12.4.7. The system auditors shall follow the reporting standard as specified in **Annexure - 4** of this Master Circular for the executive summary of the System Audit report to highlight the major findings of the System Audit.

12.5. Auditor Selection Norms

12.5.1. 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.

12.5.2. It is recommended that resources employed shall have relevant industry recognized certifications including but not limited to the following:

- 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)

12.5.3. The Auditor must possess demonstrable expertise in IT audit and governance frameworks, with experience aligned to industry-leading practices such as Control Objectives for Information and Related Technologies (COBIT).

12.5.4. The Auditor shall be free from any conflict of interest that could impair the conduct of a fair, objective and independent audit of the Broker Dealer. Further, the directors or partners of the Auditor firm shall not have any direct or indirect relationship with the Broker Dealer.

12.5.5. The Auditor must 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.

13. Early Warning Mechanism to Prevent Diversion of Client Securities

13.1. Stock Exchanges, Clearing Corporations and Depository shall develop an early warning mechanism and information sharing mechanism amongst 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 – V: DEALING WITH CLIENT

14. Unique Client Code

14.1. It shall be mandatory for the Broker Dealer to use unique client code for all clients.

15. Regulation of Transactions Between Clients and Broker Dealers

15.1. All Broker Dealers shall operate distinct, separate accounts for proprietary and client capital. The use of client funds to satisfy the Broker Dealer's proprietary obligations or principal positions is strictly prohibited. Any overlap between these accounts shall be treated as a material breach of fiduciary duty and a violation of IFSCA guidelines.

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

15.3. The Broker Dealer shall implement rigorous internal controls to ensure that client collateral is utilized exclusively for the respective client's margin obligations or settlement pay-ins. Any diversion of client collateral for proprietary use or for the benefit of other clients is strictly prohibited.

15.4. Rules 8(1)(f) and 8(3)(f) of SCRR require that members of a Stock Exchange shall not engage in any business other than that of securities (with certain exceptions being there in the SCRR for the same). Stock Exchanges shall ensure that the Broker Dealers are compliant with the requirements of the SCRR.

15.5. 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.

16. Market Access through Authorised Persons in foreign jurisdictions

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

17. **Market Access through Authorised Persons in India**

17.1. To enable access to resident Indian investors through Liberalized Remittance Scheme (LRS) route, for exchange traded securities in IFSC, IFSCA registered Broker Dealers have been permitted to provide market access to investors through Authorized Persons based in India.

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

CHAPTER – VI: TECHNOLOGY RELATED PROVISIONS

18. Electronic Contract Note (ECN)

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

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

19.1. 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 the purposes of:

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

19.2. Testing of Software

19.2.1. 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 any change to such testing facility shall be mandatory for market participants, before putting it in use.

b. Mock testing

i. The Stock Exchanges shall conduct mock trading sessions on a regular and structured basis, at a minimum frequency of once per calendar month, to enable rigorous testing of new software deployments as well as existing systems that have undergone any functional modification. Such sessions shall be executed in a controlled environment that closely replicates live trading conditions. The Stock Exchanges shall be responsible for the comprehensive design, planning and execution of these sessions, with a specific mandate to ensure broad-based market participation and the generation of adequate trading volumes. The objective shall be to facilitate robust, end-to-end validation of system performance, resilience and market integrity under conditions that mirror actual trading scenarios.

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

iii. In order to enhance the effectiveness and diagnostic value of mock trading sessions, participation shall be mandatory for all Broker Dealers authorized to undertake Algorithmic Trading.

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. 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.

iii. 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.

19.2.2. 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.

19.2.3. The Stock Exchanges shall actively monitor and ensure compliance by Broker Dealers utilizing trading algorithms with the mandatory participation requirements in mock trading sessions as specified herein. In those instances where a Broker Dealer fails to participate in such sessions, the Stock Exchange shall seek a written explanation for the non-compliance. Where the explanation provided by the Broker Dealer is found to be unsatisfactory, the Stock Exchange shall initiate appropriate regulatory or disciplinary action against the concerned Broker Dealer.

19.2.4. The Stock Exchanges shall also ensure that the system auditors examine the compliance of Broker Dealer, who uses 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 indicates 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 the reasons are found to be unsatisfactory, the Stock Exchange shall take necessary action against such Broker Dealer.

19.2.5. For pre-approval / periodic system audit of API, 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, the Broker Dealer 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.

19.3. Approval of Software of Broker Dealer

19.3.1. The Broker Dealer shall obtain prior approval from the respective Stock Exchange(s) before deploying any software in the securities market. Such an approval shall be sought by submitting all the requisite information, including details of the software, testing undertaken, and the certificate/report issued by the system auditor. The Stock Exchange may, at its discretion, seek additional information or documentation as deemed necessary for a comprehensive evaluation of the Broker Dealer's application.

19.3.2. The Stock Exchange shall examine the application submitted by the Broker Dealer and upon such examination, either grant approval or reject the application, as the case may be. The decision shall be communicated to the Broker Dealer within fifteen working days from the date of receipt of a complete application, or within such other timeframe as may be specified by IFSCA. In the event of rejection, the Stock Exchange shall, within the same stipulated period, communicate the reasons for such rejection to the Broker Dealer.

19.3.3. Prior to granting approval for the deployment of any software in the securities market, the Stock Exchange shall satisfy itself that the Broker Dealer has fully complied with all the applicable requirements and standards specified by the IFSCA and/or the Stock Exchange in respect of such software.

19.3.4. The Stock Exchange may appropriately structure and sequence the requirements relating to mock testing, certification of test reports by system

auditor(s) and the software approval process, with a view to enabling expeditious approvals and ensuring a seamless transition of a Broker Dealer to new or upgraded software.

19.3.5. To ensure that the Broker Dealer does not deploy or operate software without obtaining the requisite approvals, the Stock Exchange shall establish and maintain robust control mechanisms to detect and prevent any unauthorized modifications to the approved software.

19.4. Undertaking to be provided by Broker Dealers

19.4.1. The Broker Dealer shall submit an undertaking to the respective Stock Exchange stating the following at the minimum:

a. M/s (name of the Broker Dealer) shall 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 shall be tested as per the framework specified by IFSCA/Stock Exchange before deployment of such new/modified software in securities market;
b. M/s (name of the Broker Dealer) shall ensure that approval of the Stock Exchange is sought for all new/modified software and shall comply with various requirements specified by IFSCA/Stock Exchange from time to time with regard to usage, testing and audit of the software; and
c. The absolute liability arising from failure to comply with the above provisions shall lie entirely with M/s (name of the Broker Dealer)

19.4.2. The Stock Exchange may include additional clauses, as deemed necessary, in the undertaking.

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

19.5.1. 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.

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

19.5.1.2. In case of refusal to share APIs, the Stock Exchange shall give 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.

19.5.1.3. 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.

19.6. Penalty on malfunction of software used by Broker Dealer

19.6.1. The Stock Exchanges shall investigate instances of software malfunction involving systems deployed by the Broker Dealer and where warranted, apply deterrent penalties in the form of fines or suspension of the Broker Dealer. Further, Broker Dealers shall institute robust risk mitigation and control mechanisms, including but not limited to the following, to limit potential losses arising from any software malfunction:

a) Broker Dealers shall incorporate appropriate contractual provisions in their agreements with software vendors clearly delineating the respective rights, obligations and liabilities of the software vendor and the Broker Dealer in the event of any software malfunction; and/ or
b) Broker Dealers shall evaluate and where deemed appropriate, obtain adequate insurance coverage to mitigate potential losses arising from software malfunctions.

19.7. With regard to changes/updates to the Broker Dealer's 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 Exchange.

19.8. The Stock Exchange shall direct its 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.

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

20.1. 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 a timely and continuous manner may create a situation of stress in the securities market.

20.2. Broker Dealers shall establish Vendor Transition Protocols that ensure that the entity can migrate its trading and clearing functions to another software vendor without data loss or operational downtime.

20.3. To ensure the continuity of market operations, the Stock Exchange may advise the Broker Dealers to undertake the following measures:

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

20.3.2. In case of large Broker Dealers, adopt a multi-vendor strategy for their core trading and risk management engines. This diversification is necessary to eliminate "single points of failure" and ensure the systemic stability of the securities market in the IFSC.

20.3.3. Consider including the following enforceable covenants in their contracts with the software vendors to mitigate operational and systemic risk:

a) An unconditional right to access all design, development and architectural specifications if the vendor fails to maintain service continuity, ensuring that the Broker Dealer can sustain operations independently.

b) A mandatory requirement for the vendor to provide comprehensive technical training and certification to the Broker Dealer's internal staff to ensure self-sufficiency in software usage and basic maintenance.
c) Financial penalties calibrated to the severity of the system downtime or software malfunctions caused by the vendor.
d) Obligation for the vendor to provide full cooperation during regulatory, internal or forensic audits/ investigations, including access to logs and source code environments upon request.

21. Cyber Security and Cyber Resilience

21.1. In terms of regulation 21 of the CMI Regulations, the Broker Dealer/Clearing Member is required to a have robust cyber security and cyber resilience framework in accordance with the requirements as specified by the Authority from time to time.

21.2. The Broker Dealer/Clearing Member shall comply with the guidelines specified through Circular No. IFSCA-CSD0MSC/13/2025-DCS, titled "*Guidelines on Cyber Security and Cyber Resilience for Regulated Entities in IFSCs*" dated March 10, 2025, issued by the Authority. As mentioned in the said circular, the implementation of the Guidelines shall be undertaken in accordance with the principle of proportionality, after taking into due consideration:

- scale and complexity of operations;
- nature of the activity the entity is engaged in;
- interconnectedness with the financial ecosystem; and
- the corresponding cyber risks the entity is exposed to.

22. Reporting for Artificial Intelligence (AI) and Machine Learning (ML) applications and systems offered and used by Broker Dealers

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

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

23.1. Technology related interruptions and system glitches ("technical glitches"), and their consequent impact on investors' ability to access and execute trades, constitute a significant source of operational and market risk. Accordingly, the following framework for identification, reporting, mitigation and resolution of technical glitches in the trading systems of Broker Dealers shall be strictly complied with.

23.2. Definition of a Technical Glitch

A "Technical Glitch" shall mean any failure, interruption or malfunction, irrespective of cause, affecting the operational infrastructure of a Broker Dealer. This shall include, but not be limited to, defects or errors in hardware, software, network connectivity, automated processes, and any electronic products, platforms, or services operated by the Broker Dealer.

The failure/interruption/malfunction experienced may be 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.

23.3. Reporting Requirements

23.3.1. The Broker Dealer shall report any technical glitch to the Stock Exchange forthwith upon occurrence and in any event, no later than one hour from the time of such occurrence.

23.3.2. The Broker Dealer 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.

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

23.3.4. The RCA Report submitted by the Broker Dealer shall, inter-alia, comprehensively capture the following details pertaining to the technical glitch:

- time of occurrence;
- duration;
- detailed chronology of events; and
- impact assessment.

The report shall clearly identify the cause of the technical glitch, including the root cause attributable to vendor(s), where applicable, and provide full particulars of corrective and preventive actions taken or proposed, as well as the status and manner of restoration of normal operations.

23.3.5. The Broker Dealer shall submit information stated in para 23.3.1, 23.3.2 and 23.3.3 above, to the Stock Exchanges in which the Broker Dealer is a member.

23.3.6. All technical glitches reported by the 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.

23.4. Capacity Planning

23.4.1. To ensure uninterrupted market access during periods of high volatility or client growth, the Broker Dealer shall implement a formal capacity planning framework. This framework must ensure that the entire trading ecosystem including server processing power, network bandwidth, and application throughput is provisioned to handle peak loads. Capacity planning shall be deemed a non-negotiable prerequisite for maintaining the continuity of regulated services.

23.4.2. The Broker Dealer shall monitor the throughput of their trading applications, servers and network architecture. The "Peak Load" for any given period shall be defined as the highest recorded stress point during a calendar quarter. To ensure systemic stability, Broker Dealers shall maintain an installed capacity of at least 150% (1.5x) of this observed peak load.

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

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

23.4.5. The Stock Exchange shall issue detailed guidelines on the periodicity and methodology for capacity planning, including the assessment of existing system capacity, peak load conditions and the determination of incremental capacity requirements to effectively address anticipated future system loads.

23.5. Software testing and change

23.5.1. To mitigate the risk of operational failure, the Broker Dealers shall follow a rigorous software testing and release mechanism. All software modifications, updates or patches shall undergo comprehensive validation in a non-production environment prior to deployment. No change shall be promoted to the production system without adequate tests. Recognizing that unverified software updates pose a material threat to the systems of the Broker Dealer and to market stability at large, the following shall be followed:

a. The Broker Dealer shall maintain dedicated, isolated testing environments that functionally mirrors its production systems for all software, whether developed in-house or by third-party vendors. The Software Development Life Cycle (SDLC) must incorporate Automated Unit Testing, Regression Testing, and Comprehensive Security Vulnerability Assessments.

b. Specified Broker Dealers are required to maintain fully automated testing environments. Manual testing is deemed insufficient for the complexity of high-frequency or high-volume trading system.

c. For all proprietary or vendor-supplied trading software, the Broker Dealer shall maintain a Requirements Traceability Matrix (RTM). This matrix shall explicitly map every business functionality to its corresponding unit and regression tests.

d. The Broker Dealer 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. All infrastructure including servers, Operating Systems, databases, firewalls and IDS/IPS shall be maintained at the latest stable version and patched against known vulnerabilities.

f. The Stock Exchange shall issue the necessary technical guidelines to standardize the implementation of automated testing, traceability and change management across all Broker Dealers.

23.6. Monitoring mechanism

23.6.1. The Broker Dealers shall monitor key systems & functional parameters to ensure that their trading systems function in a smooth manner. The Stock Exchange shall identify the key parameters in consultation with the Broker Dealers. These key parameters shall be monitored by Broker Dealers and by the Stock Exchange, on a real time or on a near real time basis.

23.6.2. The Stock Exchanges shall have necessary arrangements in place for monitoring the key parameters and the technical glitches occurring in the Broker Dealers' trading systems.

23.6.3. The Broker Dealers and the 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.

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

23.7.1. The Broker Dealers as identified by the Stock Exchanges based on parameters such as client base, scale of operations, or any other criteria specified from time to time, shall mandatorily establish and maintain robust Business Continuity and Disaster Recovery (BCP-DR) infrastructure.

23.7.2. The Broker Dealers shall formulate, implement and maintain a comprehensive BCP-DR policy document, clearly defining standard operating procedures to be invoked in the event of a disruption or disaster. The policy shall incorporate a continuous monitoring framework for assessing the health, resilience and performance of critical systems during normal operations and shall be subject to periodic review and strengthening to minimize risks to business continuity.

23.7.3. The DRS shall, to the extent feasible, be located in a different seismic zone from the Primary Data Centre (PDC). Where such geographic separation is not practicable due to operational constraints, the PDC and DRS shall be situated at a minimum distance of 250 kilometres from each other to mitigate the risk of concurrent disruption from the same natural disaster. The architecture shall ensure seamless and secure data synchronization between the PDC and DRS.

23.7.4. Operations undertaken by a Broker Dealer/Clearing Member, from its respective DR site located within India but outside IFSC, shall be deemed to have been conducted within IFSC.

23.7.5. Specified Broker Dealers shall mandatorily conduct DR drills including live trading from the DRS, for at least one full trading day. The frequency and scheduling of such drills shall be determined by the Stock Exchange in consultation with the concerned Broker Dealers, with the objective of ensuring operational readiness under stress conditions.

23.7.6. The Broker Dealer shall constitute designated governance and response teams empowered to take timely decisions regarding invocation of BCP, migration of operations from the PDC to the DRS, allocation of resources at the DRS and restoration of full operational capability.

23.7.7. The hardware, system software, application environment, network and security devices and associated application environments at the DRS shall maintain full parity and one-to-one correspondence with that of the PDC. The

Broker Dealer shall ensure that adequate capacity and resources are available, at all times, to support uninterrupted operations from either site.

23.7.8. The Stock Exchange, in consultation with Broker Dealers, shall prescribe Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), defining the maximum permissible time for restoration of operations and the maximum tolerable data loss, respectively, in the event of a disaster.

23.7.9. The replication architecture, network bandwidth and system load configuration between the DRS and PDC shall be engineered to meet the stipulated RTO and RPO requirements. The overall system design shall ensure high availability, optimal capacity utilization and elimination of single points of failure. All updates and data changes at the PDC shall be replicated to the DRS on a near real-time basis.

23.7.10. Specified Broker Dealers shall obtain relevant ISO certifications as may be specified by the Stock Exchange, covering IT systems and IT-enabled infrastructure and processes.

23.7.11. The System Auditor, as a part of the mandated annual System Audit, shall evaluate the adequacy and effectiveness of the BCP-DR framework, including the readiness of the Broker Dealer to transition operations from the PDC to the DRS. The auditor shall also review and provide observations on the outcomes of DR drills conducted during the audit period.

23.7.12. The Stock Exchange shall define key terms such as “critical systems” and “disaster” and issue detailed operational guidelines covering, inter alia, periodic review of BCP policies, conduct of DR drills/live trading, activation protocols for DRS and timelines for compliance with certification requirements.

23.8. The Stock Exchange shall establish and enforce a structure of financial disincentives, including graded penalties, for the Broker Dealers, in respect of technical glitches in their trading systems, and any non-compliance with the provisions set out herein.

23.9. To promote transparency, accountability and market integrity, the Stock Exchanges shall ensure public dissemination, on their respective websites, of all the instances of technical glitches in the trading systems of the Broker Dealers, along with the corresponding Root Cause Analysis (RCA).

CHAPTER – VII: INTERNAL POLICY ON OUTSOURCING OF ACTIVITIES

24. Internal Policy on Outsourcing

24.1. In terms of Code of Conduct specified under Schedule II of the CMI Regulations, the Broker Dealer/Clearing Member is required to have an internal policy for outsourcing of its activities from outside of the IFSC.

24.2. Prior to commencement of operations, every Broker Dealer/Clearing Member shall implement the internal policy for outsourcing, which shall be duly approved by its Governing Board. This policy must define the criteria for selecting service providers and the mechanisms for continuous oversight. The Broker Dealer/Clearing Member shall be principally accountable for all outsourced functions.

CHAPTER – VIII: COMPLAINT HANDLING AND GRIEVANCE REDRESSAL

25. Complaint Handling and Grievance Redressal

25.1. Regulation 18 of the CMI Regulations requires that the Broker Dealers/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.

25.2. The Broker Dealer/Clearing Member shall comply with the applicable norms and requirements relating to handling of consumer complaints specified by the Authority by way of Circular No. IFSCA-LPRA/3/2024-Legal and Regulatory Affairs, titled "*Complaint Handling and Grievance Redressal by Regulated Entities in the IFSC*", dated December 02, 2024, read with Circular No. IFSCA-LPRA/3/2024-Legal and Regulatory Affairs, 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*", dated January 13, 2025.

CHAPTER – IX: CHANGE IN CONTROL

26. Broker Dealer/Clearing Member operating in the IFSC in Branch Structure

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

26.2. **Broker Dealer/Clearing Member incorporated in the IFSC**

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

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

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

26.3.1. The Broker Dealer/Clearing Member 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 /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/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; and

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

CHAPTER – X: PERIODIC REPORTING TO THE IFSCA BY BROKER DEALER/CLEARING MEMBER

27. Quarterly Reporting

27.1. The Broker Dealer/Clearing Member shall submit reports to the respective Stock Exchange/Clearing Corporation on a quarterly basis in accordance with the requirements specified in Circular No. 1/IFSCA/CMI Supervision/2023-24, titled "*Reporting Norms for Capital Market Intermediaries in IFSC*", dated April 08, 2026 (as amended from time to time).

27.2. The Stock Exchanges/Clearing Corporations shall provide information submitted in the quarterly reports by Broker Dealers / Clearing Members in the manner and format as specified by the Authority.

28. Annual Compliance Audit

28.1. In terms of regulation 25 of the CMI Regulations, the Broker Dealer/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.

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

28.3. It is also clarified that the Broker Dealer/Clearing Member shall also submit a copy of such audit report to the Stock Exchange/Clearing Corporation. The Stock Exchange/Clearing Corporation shall be required to submit a summary of audit findings along with its recommendations to IFSCA by 30th of November of every year.

28.4. The Auditor may perform annual compliance audit of the Broker Dealer /Clearing Member for a maximum period of three years. Such an auditor / audit firm can be reappointed only after a cooling off period of 2 years.

28.5. 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 – XI: SURRENDER OF REGISTRATION

29. Surrender of Registration

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

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

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

a) Details of registration;
b) Original Certificate of Registration (if issued in physical form);
c) List of all activities that are being carried out by the entity;
d) Details of registration in any other capacity with IFSCA;
e) List of controlling shareholders and directors;
f) Details of any material regulatory action taken or pending against the Broker Dealer/Clearing Member or any of its controlling shareholder or director by any financial sector regulator in the last three years;
g) Details of ongoing material litigations, if any;
h) Copies of board resolution and shareholder resolution, as applicable, relating to surrender of registration;
i) Reasons for surrender of registration; and
j) 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.	

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

30.1. On approval of application for surrender of Broker Dealer's /Clearing Member's registration by IFSCA, the Stock Exchange/Clearing Corporation shall release Security Deposit of the Broker Dealer (engaged in trading on behalf of clients)/ Clearing Member (clearing the trades of other Broker Dealer/Remote Trading Participant) after twelve months from the date of approval of surrender application by IFSCA.

Provided that in case of a Broker Dealer engaged only in proprietary trading / Clearing Member clearing the trades for itself (self - clearing member), for the last three years prior to the date of application of surrender, security deposit shall be released 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 well documented 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 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 maintains 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

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

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

2.1.1. **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.

2.1.2. **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.

2.1.3. **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.

2.1.4. **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.

2.1.5. **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.

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

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

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

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

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

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

2.2.5. Development / Test / Production environment segregation.

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

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

2.2.8. 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.

2.3. Risk Management System (RMS)

2.3.1. **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.

2.3.2. **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.

2.3.3. **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.

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

2.3.5. **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.

2.3.6. **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.

2.4. Password Security

2.4.1. **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.

2.4.2. **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.

2.4.3. **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.

2.5. Session Management

2.5.1. **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.

2.5.2. **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.

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

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

2.6. Database Security

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

2.6.2. **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.

2.7. Network Integrity

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

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

2.7.3. **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.

2.8. Access Controls

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

2.8.2. **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.

2.9. Backup and Recovery

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

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

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

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

2.10.1. **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.

2.10.2. **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).

2.10.3. **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.

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

2.11. **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.

2.12. Back office data

2.12.1. **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.

2.12.2. **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.

2.13. User Management

2.13.1. **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.

2.13.2. **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.

2.13.3. **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.

2.13.4. **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.

2.14. **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))

2.14.1. **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.

2.14.2. **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.

2.14.3. **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.

2.14.4. **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.

2.15. **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.

2.16. **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:

2.16.1. **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.

2.16.2. **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

3. ToR for Type III Broker

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

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

3.1.2. **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.

3.1.3. **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.

3.1.4. **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.

3.1.5. **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.

3.1.6. **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.

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

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

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

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

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

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

3.2.5. Development / Test / Production environment segregation.

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

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

3.2.8. 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.

3.3. Risk Management System (RMS)

3.3.1. **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.

3.3.2. **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.

3.3.3. **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.

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

3.3.5. **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.

3.3.6. **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.

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

3.4.1. **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.

3.4.2. **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.

3.4.3. **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.

3.4.4. **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.

3.4.5. **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.

3.4.6. **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.

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

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

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

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

iv. Whether changes to the control parameters have been made by authorized users as per the Access Matrix. The system auditor should specifically comment on the reasons and frequency for changing of such control parameters. Further, the system auditor should also comment on the possibility of such tweaking leading to run away/loop situation.

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

3.4.8. **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.

3.4.9. **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.

3.5. Password Security

3.5.1. 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.

3.5.2. 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.

3.5.3. 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.

3.6. Session Management

3.6.1. **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.

3.6.2. **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.

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

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

3.7. Database Security

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

3.7.2. **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.

3.8. Network Integrity

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

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

3.8.3. **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.

3.9. Access Controls

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

3.9.2. **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.

3.10. Backup and Recovery

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

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

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

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

3.11.1. **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.

3.11.2. **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).

3.11.3. **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.

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

3.11.5. **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.

3.12. Back office data

3.12.1. **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.

3.12.2. **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.

3.13. User Management

3.13.1. **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.

3.13.2. **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.

3.13.3. **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.

3.13.4. **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.

3.14. **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))

3.14.1. **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.

3.14.2. **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.

3.14.3. **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.

3.14.4. **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.

3.15. **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.

3.15.1. **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

3.15.2. **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.

3.15.3. **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.

3.15.4. **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:

   3.a Non-Compliant

   3.b Work In progress

   3.c Observation

   3.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 above.

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

***