

## CHAPTER 2: TRADING SOFTWARE AND TECHNOLOGY

<b>1. INTERNET TRADING</b> .....	<b>4</b>
1.1. Conditions to be met by Broker for providing Internet Based Trading Service.....	4
1.2. Securities Trading through Wireless medium on Wireless Application Protocol (WAP) platform.....	8
1.3. Securities Trading using Wireless Technology.....	10
1.4. Additional Requirements for Internet Based Trading (IBT) and Securities trading using Wireless Technology (STWT).....	11
<b>2. DIRECT MARKET ACCESS FACILITY</b> .....	<b>13</b>
<b>3. ELECTRONIC CONTRACT NOTE</b> .....	<b>17</b>
3.1. Use of Digital Signature on Contract Notes.....	17
3.2. Issuance of Contract Notes in electronic form.....	17
3.3. Electronic issuance of contract notes – Additional conditions.....	17
3.4. Format for Issuance of Electronic Contract Notes.....	20
<b>4. STRAIGHT THROUGH PROCESSING</b> .....	<b>21</b>
4.1. Mechanism.....	21
4.2. The system flow of the STP framework.....	21
4.3. SEBI (STP centralised hub and STP service providers) Guidelines, 2004.....	22
4.4. Work flow for institutional investors.....	23
4.5. Clarification.....	26
4.6. Modifications in the prescribed messaging formats.....	27
<b>5. TRADING TERMINALS</b> .....	<b>29</b>
5.1. Testing of software used in or related to Trading and Risk Management.....	29
5.2. Standing Committee.....	34
5.3. Expansion of trading terminals of the Exchange.....	35
5.4. Broad Guidelines for opening Trading Terminals abroad.....	35
5.5. Safeguards to avoid trading disruption in case of failure of software vendor.....	38
<b>6. SMART ORDER ROUTING</b> .....	<b>39</b>
6.1. Introduction of Smart Order Routing.....	39
<b>7. ALGORITHMIC TRADING</b> .....	<b>42</b>
7.1. Broad Guidelines on Algorithmic Trading.....	42

<b>8.</b>	<b>ANNUAL SYSTEM AUDIT.....</b>	<b>47</b>
8.1.	System and Network Audit of Market Infrastructure Institutions (MIIs) .....	47
8.2.	Annual System Audit of Stock Brokers.....	48
8.3.	System Audit of Professional Clearing Members (PCMs).....	48
8.4.	Advisory on System and Network Audit of MIIs.....	49
<b>9.</b>	<b>BUSINESS CONTINUITY PLAN AND DISASTER RECOVERY.....</b>	<b>51</b>
9.1.	Guidelines for Business Continuity Plan (BCP) and Disaster Recovery (DR) of Market Infrastructure Institutions (MIIs) .....	51
9.2.	Business Continuity Plan (BCP) and Disaster Recovery (DR) framework – Limited Purpose Clearing Corporation (LPCC).....	55
9.3.	Standard Operating Procedure for handling of technical glitches by Market Infrastructure Institutions (MIIs) and payment of “Financial Disincentives” thereof.....	55
9.4.	Measures to strengthen tracking and reporting of delay in pay-in/pay-out for rolling settlement.....	56
9.5.	Advisory on Security Patch Management Policy.....	58
9.6.	Standard Operating Procedure for handling of Stock Exchange Outage and extension of trading hours thereof.....	58
9.7.	Testing Framework for the Information Technology (IT) Systems of the Market Infrastructure Institutions (MIIs).....	62
9.8.	Business Continuity for Clearing Corporations through Software as a Service (SaaS) Model.....	64
<b>10.</b>	<b>CYBER SECURITY AND CYBER RESILIENCE.....</b>	<b>68</b>
10.1.	Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporations and Depositories .....	68
10.2.	Cyber Security and Cyber Resilience framework – Limited Purpose Clearing Corporation (LPCC).....	68
10.3.	Strengthening Resiliency of Websites of Stock Exchanges, Clearing Corporations and Depositories (MIIs) .....	68
10.4.	Bolstering Cyber Resiliency .....	69
10.5.	Comprehensive Review of Cyber Security at Stock Exchanges, Clearing Corporations and Depositories (MIIs) .....	70
10.6.	Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporations and Depositories .....	70
10.7.	Cyber Security Operations Center for SEBI registered intermediaries.....	75

10.8.	Reporting for Artificial Intelligence (AI) and Machine Learning (ML) applications and systems offered and used by Market Infrastructure Institutions (MIIs).....	75
10.9.	Standard Operating Procedure for reporting of Cyber Security breaches, incidents and deficiencies and for imposition of “Financial Disincentive” on Market Infrastructure Institutions (MIIs) .....	76
10.10.	Implementation of Cyber Capability Index.....	80
10.11.	Advisory on Cyber Audit and VAPT .....	80
10.12.	Guidelines for MIIs regarding Cyber security and Cyber resilience .....	81
10.13.	Advisory on Encryption of Data at Rest and Data in Motion.....	81
10.14.	Advisory on Cyber security and Cyber resilience.....	82
10.15.	Measures taken to strengthen the cyber resilience of MIIs.....	83
10.16.	Patch Management Policy of MIIs.....	83
<b>11.</b>	<b>CO-LOCATION / PROXIMITY HOSTING .....</b>	<b>84</b>
11.1.	Co-location / proximity hosting facility offered by stock exchanges.....	84
11.2.	Measures to strengthen Algorithmic Trading and Co-location/ proximity Hosting Framework.....	85
11.3.	Review of guidelines for Co-location / proximity hosting facility offered by stock exchanges .....	88
<b>12.</b>	<b>CAPACITY PLANNING .....</b>	<b>90</b>
12.1.	Capacity planning framework of stock exchanges and clearing corporations .....	90
<b>13.</b>	<b>DATA FEEDS .....</b>	<b>91</b>
13.1.	Fair and transparent access to data feeds of the stock exchanges .....	91
<b>14.</b>	<b>ADVISORIES RELATED TO TECHNOLOGY .....</b>	<b>92</b>
14.1.	Advisory on Technology related Investments and Planning by Market Infrastructure Institutions (MIIs).....	92
14.2.	Advisory on automation/review of operational processes involving IT systems of Market Infrastructure Institutions (MIIs).....	93
14.3.	Process for freezing/un-freezing of accounts/holdings pursuant to issuance of orders of SEBI/ Securities Appellate Tribunal (SAT)/ Supreme Court of India/ other courts.....	94
14.4.	Segregation of IT Infrastructure and activities between stock exchanges and clearing corporations.....	96
<b>15.</b>	<b>REFERENCE: List of Circulars .....</b>	<b>97</b>

## 1. INTERNET TRADING

### 1.1. Conditions to be met by Broker for providing Internet Based Trading Service<sup>1</sup>

1.1.1. To provide Internet Based Trading Service, the broker will be required to apply to the respective stock exchange for a formal permission. The stock exchange should grant approval or reject the application as the case may be, and communicate its decision to the member within 7 calendar days of the date of completed application submitted to the exchange.

1.1.2. However before giving permission to broker to start internet based services, stock exchange shall ensure that the broker meets the minimum conditions/ criteria mentioned in this Chapter of Master Circular for Stock Exchanges and Clearing Corporations. The criteria are mentioned as below:

#### 1.1.2.1. Net worth Requirement

The broker must have a minimum net worth of Rs.50 lacs if the broker is providing the Internet based facility on his own. However, if some brokers collectively approach a service provider for providing the internet trading facility, net worth criteria as stipulated by the stock exchange will apply. The net worth shall be computed in the manner as follows:

- Capital + Free Reserves
- Less non-allowable assets viz.,
  - a) Fixed assets
  - b) Pledged securities
  - c) Member's card
  - d) Non-allowable securities (unlisted securities)
  - e) Bad deliveries
  - f) Doubtful debts and advances\*
  - g) Prepaid expenses, losses
  - h) Intangible assets
  - i) 30% of marketable securities

\* Explanation - Includes debts/advances overdue for more than three months or given to associates.

---

<sup>1</sup> Circular No. SMDRP/POLICY/CIR- 06/2000 dated January 31, 2000 and Circular No. SEBI/HO/MRD/TPD-1/P/CIR/2024/68 dated May 30, 2024

#### 1.1.2.2. **Operational and System Requirements:**

- 1.1.2.2.1. **Operational Integrity** - The Stock Exchange must ensure that the system used by the broker has provision for security, reliability and confidentiality of data through use of encryption technology. (Basic minimum security standards are specified in following paras). The Stock Exchange must also ensure that records maintained in electronic form by the broker are not susceptible to manipulation.
- 1.1.2.2.2. **System Capacity** - The Stock Exchange must ensure that the brokers maintain adequate backup systems and data storage capacity. The Stock Exchange must also ensure that the brokers have adequate system capacity for handling data transfer, and arranged for alternative means of communications in case of Internet link failure.
- 1.1.2.2.3. **Qualified Personnel** - The Stock Exchange must lay down the minimum qualification for personnel to ensure that the broker has suitably qualified and adequate personnel to handle communication including trading instructions as well as other back office work which is likely to increase because of higher volumes.
- 1.1.2.2.4. **Written Procedures - Stock Exchange must develop uniform written procedures** to handle contingency situations and for review of incoming and outgoing electronic correspondence.
- 1.1.2.2.5. **Signature Verification/ Authentication** - It is desirable that participants use authentication technologies. For this purpose, it should be mandatory for participants to use certification agencies as and when notified by Government / SEBI. They should also clearly specify when manual signatures would be required.

#### 1.1.2.3. **Client Broker Relationship**

- 1.1.2.3.1. **Know Your Client** - The Stock Exchange must ensure that brokers comply with all requirements of "Know Your Client" and have sufficient, verifiable information about clients, which would facilitate risk evaluation of clients.
- 1.1.2.3.2. **Broker-Client Agreement** - Brokers must enter into an agreement with clients spelling out all obligations and rights. This agreement should also include inter alia, the minimum service standards to be maintained by the broker for such services specified by SEBI/Exchanges for the Internet based trading from time to time. Exchanges shall prepare a model agreement for

this purpose. The broker's agreement with clients should not have any clause that is less stringent/contrary to the conditions stipulated in the model agreement prepared by the Exchanges for this purpose.

- 1.1.2.3.3. **Investor Information** - The broker web site providing the internet based trading facility should contain information meant for investor protection such as rules and regulations affecting client broker relationship, arbitration rules, investor protection rules etc. The broker web site providing the Internet based trading facility should also provide and display prominently, hyper link to the web site/ page on the web site of the relevant stock exchange(s) displaying rules/ regulations/circulars. Ticker/quote/order book displayed on the web-site of the broker should display the time stamp as well as the source of such information against the given information.
- 1.1.2.3.4. **Order/Trade Confirmation** - Order/Trade confirmation should also be sent to the investor through email at client's discretion at the time period specified by the client in addition to the other mode of display of such confirmations on real time basis on the broker web site. The investor should be allowed to specify the time interval on the web site itself within which he would like to receive this information through email. Facility for reconfirmation of orders which are larger than that specified by the member's risk management system should be provided on the internet based system.
- 1.1.2.3.5. **Handling Complaints by Investors** - Exchanges should monitor complaints from investors regarding service provided by brokers to ensure a minimum level of service. Exchanges should have separate cell specifically to handle Internet trading related complaints and should also have facility for on-line registration of complaints on their web-site.

#### 1.1.2.4. **Risk Management**

- 1.1.2.4.1. Exchanges must ensure that brokers have a system-based control on the trading limits of clients, and exposures taken by clients. Brokers must set pre-defined limits on the exposure and turnover of each client.
- 1.1.2.4.2. The broker systems should be capable of assessing the risk of the client as soon as the order comes in. The client should be informed of acceptance/rejection of the order within a reasonable period. In case system based control rejects an order because of client having exceeded limits etc., the broker system may have a review and release facility to allow the order to pass through.

1.1.2.4.3. Reports on margin requirements, payment and delivery obligations, etc. should be informed to the client through the system.

**1.1.2.5. Contract Notes**

Contract notes must be issued to clients as per existing regulations, within 24 hours of the trade execution.

**1.1.2.6. Cross Trades**

As in the case of existing system, brokers using Internet based systems for routing client orders will not be allowed to cross trades of their clients with each other. All orders must be offered to the market for matching.

**1.1.2.7. Network Security Protocols and Interface Standards**

**1.1.2.7.1. Network Security -**

The following security features are mandatory for all Internet based trading systems:

- i. User id
- ii. First Level password (Private code)
- iii. Automatic expiry of passwords at the end of a reasonable duration. Reinitialise access on entering fresh passwords.
- iv. All transaction logs with proper audit facilities to be maintained in the system.
- v. Secured Socket Level Security for server access through Internet
- vi. Suitable Firewalls between trading set-up directly connected to and Exchange trading system and the Internet trading set-up.

The following advanced security products are advisable.

- a. Microprocessor based SMART cards
- b. Dynamic Password (Secure ID Tokens)
- c. 64 bit/128 bit encryption \*\*
- d. Second Level password (personal information e.g. village name, birth date etc.)

\*\*DOT policy and regulations will govern the level of encryption.

**1.1.2.7.2. Standards for Web Interfaces and Protocols -**

Between a Trading Web Server and Trading Client Terminals, Interfaces Standards as per recommendations of IETF (Internet Engineering Task Force)

and W3C (World Wide Web Consortium) may be adopted. E.g.: HTTP Ver 4 or above HTML Ver 4/XML.

#### 1.1.2.7.3. **Systems Operations -**

- a. Brokers should follow the similar logic/priorities used by the Exchange to treat client orders.
- b. Brokers should maintain all activities/ alerts log with audit trail facility.
- c. Broker Web Server should have internally generated unique numbering for all client order/trades.
- d. Brokers should seek permission from the Exchange before commencement of Internet trading facility after providing complete details of the features of implemented systems.
- e. Further, Exchanges would publish IBT statistics on the basis of details of IBT terminals provided by the stock brokers. Exchanges, in this regard, may obtain information/declaration about IBT terminals from stock brokers as deemed fit by them.

1.1.3. In addition to the requirements mentioned above, all existing obligations of the broker as per current regulations will continue without changes.

### 1.2. **Securities Trading through Wireless medium on Wireless Application Protocol (WAP) platform<sup>2</sup>**

1.2.1. A broker providing stock trading through WAP must be a SEBI registered broker who also has an Internet website which complies with all the requirements laid down by SEBI at Para 1.1 of this Chapter of Master Circular for Stock Exchanges and Clearing Corporations. Further, some additional requirements are to be met by the broker for providing securities transaction through WAP, which are as follows:

#### 1.2.1.1. **Network Security**

1.2.1.1.1. The break in data encryption at the WAP gateway server raises security issues. Until the shortcoming is addressed by WAP, the WAP server should be hosted by the broker itself and not by a third party.

1.2.1.1.2. Suitable firewalls should be installed between trading set-up directly connected to an Exchange trading system and the WAP server.

---

<sup>2</sup> Circular No. SMDRP/Policy/Cir-48/2000 dated October 11, 2000

- 1.2.1.1.3. WTLS (Wireless Transport Layer Security) level security or a higher level of security (as and when available) for wireless communication is mandatory for wireless transactions.
  - 1.2.1.1.4. The WTLS encrypts data upto the WAP Gateway server. Transmission from the WAP Gateway server to the Internet server should be secured using Secured Socket Level Security, preferably with 128 bit encryption, for server access through Internet. Alternately, the WAP Gateway server and Internet server may be co-hosted. The server resource should not be shared for any other applications.
  - 1.2.1.1.5. The following security measures applicable for fixed Internet based systems should be made mandatory:
    - 1.2.1.1.5.1. User ID
    - 1.2.1.1.5.2. First Level password (Private code)
    - 1.2.1.1.5.3. Automatic expiry of passwords at the end of a reasonable duration. Reinitialize access on entering fresh passwords
    - 1.2.1.1.5.4. All transaction logs with proper audit facilities to be maintained in the system.
  - 1.2.1.1.6. Digitally signed transactions ensure client authentication and support non-repudiation. Digital certification should be mandatory for participants as and when certification agencies are notified by Government / SEBI.
  - 1.2.1.1.7. In case of failure of the network, alternative means of communication such as telephone, Internet or e-mail should be available.
- 1.2.1.2. Price Quotes/ Order/ Trade Confirmations**
- 1.2.1.2.1. Stock quotes should be time-stamped.
  - 1.2.1.2.2. All orders and trades must be identified by a unique ID. Order confirmation must be provided to the user on submitting the order. Order modification/ cancellation facilities must also be provided. This may be provided using alternate protocols in case the same is not supported by WAP.
  - 1.2.1.2.3. Trade confirmation should be provided to the user through e-mail and/or on the mobile phone.
- 1.2.1.3. System operations**
- 1.2.1.3.1. Brokers should follow the similar logic/priorities used by the Exchange to treat client orders.

- 1.2.1.3.2. Orders/ trades placed through either fixed Internet or WAP system should be accessible from both systems.
- 1.2.1.3.3. Brokers should maintain all activities/ alerts log with audit trail facility.
- 1.2.1.3.4. Broker Web Server should have internally generated unique numbering for all client order/trades.

#### 1.2.1.4. Risk Management

- 1.2.1.4.1. It is emphasised that risk management should be comprehensive and the risk management systems should take into account the overall positions of clients, irrespective of the medium of trading.

### 1.3. Securities Trading using Wireless Technology<sup>3</sup>

- 1.3.1. It has been decided that SEBI registered brokers who provide Internet Based Trading as specified by SEBI shall be eligible to provide securities trading using wireless technology. All relevant requirements applicable to internet based trading shall also be applicable to securities trading using wireless technology.
- 1.3.2. Securities Trading using Wireless technology shall include devices such as mobile phone, laptop with data card, etc, that use Internet Protocol (IP).
- 1.3.3. In addition, the stock exchange shall ensure that the broker complies with the following:
  - 1.3.3.1. There shall be secure access, encryption and security of communication for internet based trading and securities trading using wireless technology. The policy and regulation of the Department of Telecommunications (“DOT”) shall govern the level of encryption.
  - 1.3.3.2. Adequate measures should be taken for user identification, authentication and access control using means such as user-id, passwords, smart cards, biometric devices or other reliable means, to prevent misuse of facility by unauthorized persons.
  - 1.3.3.3. Unique identification number as given in case of internet based trading shall be made applicable for securities trading using wireless technology.
  - 1.3.3.4. In case of failure of the wireless network, alternative means of communication for placing orders should be available.
  - 1.3.3.5. Additional provisions specifying possible risks, responsibilities and liabilities associated with securities trading using wireless technology should be

---

<sup>3</sup> Circular No. CIR/MRD/DP/ 25/2010 dated August 27, 2010

incorporated in the Broker-Client agreement as an addendum or by bringing to the notice of clients, who are desirous of availing such facility, and taking their concurrence on the same.

- 1.3.3.6. As it may not be possible to give detailed information to the investor on a hand held device e.g. mobile phones, it may be ensured that minimum information may be given with addresses of the Internet web site/web page where detailed information would be available.
  - 1.3.3.7. Order confirmation should be provided to the user on submitting the order. Order modification / cancellation facilities should also be provided. Trade confirmation should be provided to the user, along with history of trades for the day.
  - 1.3.3.8. Session login details should not be stored on the devices used for internet based trading and securities trading using wireless technology.
  - 1.3.3.9. Network security protocols and interface standards should be as per prevalent industry standards and sound audit trails should be available for all transactions conducted using wireless devices.
  - 1.3.3.10. The broker's server routing orders to the exchange trading system shall be located in India.
  - 1.3.3.11. Stock exchanges shall arrange for periodic systems audits of broker systems to ensure that requirements specified in the circulars are being met.
  - 1.3.3.12. Stock exchange shall also include securities trading using wireless technology in their ongoing investor awareness and educational programme
- 1.4. Additional Requirements for Internet Based Trading (IBT) and Securities trading using Wireless Technology (STWT)<sup>4</sup>**

1.4.1. The stock exchange shall ensure that the broker comply with the following:

- 1.4.1.1. The broker shall capture the IP (Internet Protocol) address (from where the orders are originating), for all IBT/ STWT orders.
- 1.4.1.2. The brokers system should have built-in high system availability to address any single point failure.
- 1.4.1.3. There should be secure end-to-end encryption for all data transmission between the client and the broker through a Secure Standardized Protocol. A procedure of mutual authentication between the client and the broker server should be implemented.

---

<sup>4</sup> Circular No. CIR/MRD/DP/08/2011 dated June 30, 2011

- 1.4.1.4. The broker system should have adequate safety features to ensure it is not susceptible to internal/ external attacks.
- 1.4.1.5. In case of failure of IBT/ STWT, the alternate channel of communication shall have adequate capabilities for client identification and authentication.
- 1.4.1.6. Two-factor authentication for login session may be implemented for all orders emanating using Internet Protocol. Public Key Infrastructure (PKI) based implementation using digital signatures, supported by one of the agencies certified by the government of India, is advisable. Further the two factors in the Two-factor authentication framework should not be same.
- 1.4.1.7. In case of no activity by the client, the system should provide for automatic trading session logout.
- 1.4.1.8. Further to the above, the following practice is advisable –
  - 1.4.1.8.1. The back-up and restore systems implemented by the broker should be adequate to deliver sustained performance and high availability. The broker system should have on-site as well as remote site back-up capabilities.

## 2. DIRECT MARKET ACCESS FACILITY<sup>5</sup>

- 2.1. Direct Market Access (“DMA”) is a facility which allows brokers to offer clients direct access to the exchange trading system through the broker’s infrastructure without manual intervention by the broker. Some of the advantages offered by DMA are direct control of clients over orders, faster execution of client orders, reduced risk of errors associated with manual order entry, greater transparency, increased liquidity, lower impact costs for large orders, better audit trails and better use of hedging and arbitrage opportunities through the use of decision support tools / algorithms for trading.
- 2.2. While ensuring conformity with the provisions of the Securities Contracts (Regulation) Act, 1956 (42 of 1956), Stock Exchanges may facilitate Direct Market Access for investors subject to the following conditions:

### 2.2.1. Application for Direct Market Access (DMA) facility

- 2.2.1.1. Brokers interested to offer DMA facility shall apply to the respective stock exchanges giving details of the software and systems proposed to be used, which shall be duly certified by a Security Auditor as reliable.
- 2.2.1.2. The stock exchange should grant approval or reject the application as the case may be, and communicate its decision to the member within 30 calendar days of the date of completed application submitted to the exchange.
- 2.2.1.3. The stock exchange, before giving permission to brokers to offer DMA facility shall ensure the fulfillment of the conditions specified hereinafter.

### 2.2.2. Operational specifications

- 2.2.2.1. All DMA orders shall be routed to the exchange trading system through the broker’s trading system. The broker’s server routing DMA orders to the exchange trading system shall be located in India.
- 2.2.2.2. The broker should ensure sound audit trail for all DMA orders and trades, and be able to provide identification of actual user-id for all such orders and trades. The audit trail data should be available for at least 5 years.
- 2.2.2.3. Exchanges should be able to identify and distinguish DMA orders and trades from other orders and trades. Exchanges shall maintain statistical data on DMA trades and provide information on the same to SEBI on a need basis.

---

<sup>5</sup> Circular No. MRD/ DoP/SE/Cir- 7 /2008 dated April 03, 2008.

- 2.2.2.4. The DMA system shall have sufficient security features including password protection for the user ID, automatic expiry of passwords at the end of a reasonable duration, and re-initialisation of access on entering fresh passwords.
- 2.2.2.5. In case where the clients access the DMA server of the broker through a third party service provider, the password maintenance and authentication can be done either by the broker or by third party network service provider, so long as the exchange/broker ensures secured access and communication and a sound audit trail for all DMA orders/ trades. The authorized user and client details should be part of the order details received and authenticated at the DMA server of the broker.
- 2.2.2.6. Brokers should follow the similar logic/priorities used by the Exchange to treat DMA client orders. Brokers should maintain all activities/ alerts log with audit trail facility. The DMA Server should have internally generated unique numbering for all such client order/trades.
- 2.2.2.7. A systems audit of the DMA systems and software shall be periodically carried out by the broker as may be specified by the exchange and certificate in this regard shall be submitted to the exchange.
- 2.2.2.8. The exchanges and brokers should provide for adequate systems and procedures to handle the DMA trades.

### 2.2.3. Terms and Conditions<sup>6</sup>

- 2.2.3.1. Exchange shall specify from time to time the categories of investors to whom the DMA facility can be extended. Currently, this facility is available for institutional clients. Brokers shall specifically authorize clients or investment managers acting on behalf of clients for providing DMA facility, after fulfilling Know Your Client requirements and carrying out necessary due diligence. The broker shall maintain proper records of such due diligence.
- 2.2.3.2. In order to bring uniformity on the requirement of documentation for trading account opening process, the specific Broker - Client Agreement for the purpose of DMA shall be replaced with the "Terms and Conditions" document as specified at Annexure I. The "Terms and Conditions" shall be provided to the client or investment manager acting on behalf of a client (s) for availing the DMA facility. In case the DMA facility provided by the stock broker is used by the client the paragraphs one to eighteen of Part A of Annexure I shall be applicable. In case the DMA facility provided by the stock

---

<sup>6</sup> Circular No. CIR/MRD/DP/20/2012 dated August 02, 2012

broker is used by the client through an investment manager the paragraphs one to eighteen of Part B of Annexure I shall be applicable and additionally, the investment manager shall provide to the stock broker the details as specified at Annexure II.

#### **2.2.4. DMA Facility through Investment Manager<sup>7</sup>**

- 2.2.4.1. The facility of DMA provided by the stock broker shall be used by the client or an investment manager of the client. A SEBI registered entity shall be permitted to act as an investment manager on behalf of institutional clients. In case the facility of DMA is used by the client through an investment manager, the investment manager may execute the necessary documents on behalf of the client(s).
- 2.2.4.2. The exchange/ broker shall ensure that proper audit trails are available to establish identity of the ultimate client.

#### **2.2.5. Risk Management**

- 2.2.5.1. The broker shall ensure that trading limits/ exposure limits/ position limits are set for all DMA clients based on risk assessment, credit quality and available margins of the client. The broker system shall have appropriate authority levels to ensure that the limits can be set up only by persons authorized by the risk / compliance manager.
- 2.2.5.2. The broker shall ensure that all DMA orders are routed through electronic/automated risk management systems of the broker to carry out appropriate validations of all risk parameters including Quantity Limits, Price Range Checks, Order Value, and Credit Checks before the orders are released to the Exchange.
- 2.2.5.3. All DMA orders shall be subjected to the following limits:
  - 2.2.5.3.1. Order quantity / order value limit in terms of price and quantity specified for the client.
  - 2.2.5.3.2. All the position limits which are specified in the derivatives segment as applicable.
  - 2.2.5.3.3. Net position that can be outstanding so as to fully cover the risk emanating from the trades with the available margins of the specific client.

---

<sup>7</sup> Circular No. MRD/ DP/20/2012 dated August 02, 2012

2.2.5.3.4. Appropriate limits for securities which are subject to limits on Foreign Portfolio Investors (“FPIs”) as specified by the Reserve Bank of India (“RBI”).

2.2.5.4. The broker may provide for additional risk management parameters as they may consider appropriate.

#### **2.2.6. Broker to be liable for DMA trades**

2.2.6.1. The broker shall be fully responsible and liable for all orders emanating through their DMA systems. It shall be the responsibility of the broker to ensure that only clients who fulfill the eligibility criteria are permitted to use the DMA facility.

#### **2.2.7. Cross Trades**

2.2.7.1. Brokers using DMA facility for routing client orders shall not be allowed to cross trades of their clients with each other. All orders must be offered to the market for matching.

#### **2.2.8. Other legal provisions**

2.2.8.1. In addition to the requirements mentioned above, all existing obligations of the broker as per current regulations and circulars will continue without change. Exchanges may also like to specify additional safeguards / conditions as they may deem fit for allowing DMA facilities to their brokers.

### 3. ELECTRONIC CONTRACT NOTE

#### 3.1. Use of Digital Signature on Contract Notes<sup>8</sup>

Pursuant to the discussions in the Secondary Market Advisory Committee (“SMAC”) and provisions of the Information Technology Act, 2000 (“IT Act, 2000”) it is clarified that the brokers are allowed to issue contract notes authenticated by means of digital signatures provided that the broker has obtained digital signature certificate from Certifying Authority under the IT Act, 2000. Mode of confirmation by the client may be as specified in the agreement between the broker and the client.

#### 3.2. Issuance of Contract Notes in electronic form<sup>9</sup>

The contract notes can be issued by the brokers in electronic form authenticated by means of digital signatures.

#### 3.3. Electronic issuance of contract notes – Additional conditions<sup>10</sup>

All the members of stock exchanges who are desirous of issuing Electronic Contract Notes (“ECNs”) to their clients shall comply with the following conditions:

##### 3.3.1. Issuing ECNs when specifically consented

The digitally signed ECNs may be sent only to those clients who have opted to receive the contract notes in an electronic form, either in the Member – Client agreement / Tripartite agreement or by a separate letter. The mode of confirmation shall be as per the agreement entered into with the clients.

---

<sup>8</sup> Circular No. SMDRP/POLICY/CIR-56/00 dated December 15, 2000

<sup>9</sup> Circular No. SEBI/SMD/SE/15/2003/29/04 dated April 29, 2003

<sup>10</sup> Circular No. MRD/DoP/SE/Cir-20/2005 dated September 8, 2005

### **3.3.2. Where to send ECNs**

The usual mode of delivery of ECNs to the clients shall be through e-mail. For this purpose, the client shall provide an appropriate e-mail account to the member which shall be made available at all times for such receipts of ECNs.

### **3.3.3. Requirement of digital signature**

All ECNs sent through the e-mail shall be digitally signed, encrypted, non-tamperable and shall comply with the provisions of the IT Act, 2000. In case the ECN is sent through e-mail as an attachment, the attached file shall also be secured with the digital signature, encrypted and non-tamperable.

### **3.3.4. Requirements for acknowledgement, proof of delivery, log report etc.**

#### **3.3.4.1. Acknowledgement**

The acknowledgement of the e-mail shall be retained by the member in a soft and non-tamperable form.

#### **3.3.4.2. Proof of delivery**

3.3.4.2.1. The proof of delivery i.e., log report generated by the system at the time of sending the contract notes shall be maintained by the member for the specified period under the extant regulations of SEBI/stock exchanges and shall be made available during inspection, audit, etc.

3.3.4.2.2. The member shall clearly communicate to the client in the agreement executed with the client for this purpose that non-receipt of bounced mail notification by the member shall amount to delivery of the contract note at the e-mail ID of the client.

#### **3.3.4.3. Log Report for rejected or bounced mails**

3.3.4.3.1. The log report shall also provide the details of the contract notes that are not delivered to the client/e-mails rejected or bounced back.

3.3.4.3.2. Also, the member shall take all possible steps (including settings of mail servers, etc.) to ensure receipt of notification of bounced mails by the

member at all times within the stipulated time period under the extant regulations of SEBI/stock exchanges.

### **3.3.5. When to issue or send in Physical mode**

#### **3.3.5.1. Issue in Physical mode**

In the case of those clients who do not opt to receive the contract notes in the electronic form, the member shall continue to send contract notes in the physical mode to such clients.

#### **3.3.5.2. Send in Physical mode**

Wherever the ECNs have not been delivered to the client or has been rejected (bouncing of mails) by the e-mail ID of the client, the member shall send a physical contract note to the client within the stipulated time under the extant regulations of SEBI/stock exchanges and maintain the proof of delivery of such physical contract notes.

### **3.3.6. General requirements**

#### **3.3.6.1. ECNs through website**

In addition to the e-mail communication of the ECNs in the manner stated above, in order to further strengthen the electronic communication channel, the member shall simultaneously publish the ECN on his designated web-site in a secured way and enable relevant access to the clients.

#### **3.3.6.2. Access to the website**

In order to enable clients to access the ECNs posted in the designated website in a secured way, the member shall allot a unique user name and password for the purpose, with an option to the client to access the same and save the contract note electronically or take a print out of the same.

3.3.6.3. Preservation/ Archive of electronic documents

The member shall retain/archive such electronic documents as per the extant rules/regulations/circulars/guidelines issued by SEBI/Stock Exchanges from time to time.

3.4. **Format for Issuance of Electronic Contract Notes<sup>11</sup>**

3.4.1. In order to streamline the issuance of electronic contract notes as a legal document like the physical contract note, the exchanges are advised to implement the following:

- 3.4.1.1. The exchanges would prescribe a standard format for the electronic contract note (based on the model format prescribed at Annexure III (for Equity) and (for Debt<sup>12</sup>) in its bye-laws, rules and regulations.
- 3.4.1.2. The exchange bye-laws, rules and regulations for issuance of electronic contract note shall be amended to include all the standard pre-printed terms and conditions in the physical contract note. The electronic contract note would mention the relevant bye-laws / rules / regulations of the exchange subject to which the said contract note is being issued.
- 3.4.1.3. The exchange shall also modify / amend other relevant bye-laws, rules and regulations with respect to signing of the electronic contract note with a digital signature so as to make the modified format of the electronic contract note a valid legal document like the physical contract note.
- 3.4.1.4. The mechanism of record keeping of electronic contract notes in a soft non-tamperable form shall be prescribed by the exchange in compliance with the provisions of the Information Technology Act, 2000.

---

<sup>11</sup> Circular No. DNP/SE/Cir-9/04 dated February 03, 2004

<sup>12</sup> Circular No. SEBI/MRD/SE/Cir-11/2004 dated February 25, 2004

## 4. STRAIGHT THROUGH PROCESSING

### 4.1. Mechanism<sup>13</sup>

4.1.1. Straight Through Processing (“STP”) is generally understood to be a mechanism that automates the end to end processing of transactions of financial instruments. It involves use of a system to process or control all elements of the work flow of a financial transaction, what are commonly known as the Front, Middle, Back office and General Ledger. In other words, STP allows electronic capturing and processing of transactions in one pass from the point of order origination to final settlement. STP thus streamlines the process of trade execution and settlement and avoids manual entry and re-entry of the details of the same trade by different market intermediaries and participants. Usage of STP enables orders to be processed, confirmed, settled in a shorter time period and in a more cost effective manner with fewer errors. Apart from compressing the clearing and settlement time, STP also provides a flexible, cost effective infrastructure, which enables e-business expansion through online processing and access to enterprise data.

4.1.2. It has been mandated that all the institutional trades executed on the stock exchanges would be processed through the STP System.

### 4.2. The system flow of the STP framework<sup>14</sup>

4.2.1. While several STP Service Providers provide STP service to the market participants to resolve the issue of inter-operability between the STP Service Providers it was decided in consultation with the stock exchanges and the STP Service Providers that a STP Centralised Hub would be setup.

4.2.2. The system flow for the STP framework shall be as follows:

4.2.2.1. STP user intending to send an instruction would send the message to his STP service provider after digitally signing the same.

4.2.2.2. The STP service provider would verify the signature of the STP user and forward it to the

- recipient STP user, if the recipient STP user is availing services of the same STP service provider or the

---

<sup>13</sup> Circular No. DNP/04 dated April 01, 2004

<sup>14</sup> Circular No. DNP/04 dated April 27, 2004

- STP centralized hub if the recipient STP user is not with the same STP service provider. In such a case the STP service provider would be required to prepare a message as per the STP centralized hub prescribed message format, enclose the user's message, digitally sign the message and then send it to the STP centralized hub.

4.2.2.3. On receipt of the message by the STP centralized hub, the STP centralized hub would:

4.2.2.3.1. verify the signature of the sending STP service provider only.

4.2.2.3.2. send an acknowledgment to the sending STP service provider.

4.2.2.4. The STP centralized hub would forward the message to the recipient STP service provider after digitally signing on the message.

4.2.2.5. The recipient STP service provider on receipt of the message from the STP centralized hub shall verify the signature of the STP centralized hub, verify if the recipient STP user is associated with it and send an appropriate acknowledgment with digital signature to the STP centralized hub. The STP centralized hub would in turn forward the acknowledgment (received from the recipient STP service provider) duly signed to the sending STP service provider.

4.2.2.6. The recipient STP service provider shall forward the message to the recipient STP user. The recipient STP user would receive the message and verify the signature of the recipient STP service provider and sending STP user.

4.2.3. To enable inter-operation, the STP centralized hub would provide a utility / client software to the STP service provider. The STP service provider's point of interface with the STP centralized hub would be through this utility / client software. The PKI (Public key infrastructure) system for the interface shall be implemented at a later stage.

4.2.4. The block diagram of the entire STP System is placed at Annexure IV.

#### 4.3. **SEBI (STP centralised hub and STP service providers) Guidelines, 2004<sup>15</sup>**

4.3.1. SEBI in order to regulate the STP service has issued the SEBI (STP centralised hub and STP service providers) Guidelines, 2004 (herein referred to as "STP

---

<sup>15</sup> Ref.No. DNPD/Cir-24/04 dated May 26, 2004 (STP Guidelines)

Guidelines”) which also prescribe the model agreement between the STP centralised hub and the STP service providers.

4.3.2. The STP guidelines specify the eligibility criteria and conditions of approval for the STP centralised hub and the STP service providers, obligations and responsibilities of the STP centralised hub and the STP service providers and code of conduct for the STP service providers. The STP centralised hub and the STP service providers shall abide by these Guidelines.

4.3.3. To prescribe contractual obligations between the STP centralised hub and the STP service providers and to facilitate standardisation of service, a model agreement between the STP centralised hub and the STP service providers has also been prescribed by SEBI and is prescribed as Schedule II of the STP Guidelines. The agreement between the STP centralised hub and the STP service provider shall include the provisions included in the model agreement.

#### 4.4. **Work flow for institutional investors<sup>16</sup>**

4.4.1. SEBI in consultation with the STP centralized hub, STP service providers and the STP users has prescribed the transaction work flow for the STP system. All institutional investors shall follow the following transaction work flow on a mandatory basis:

4.4.1.1. A contract note in electronic form in the prescribed format (IFN 515 messaging format) shall be issued by the broker & sent to the custodian and/ or the institutional investor.

4.4.1.2. In case the contract note is processed directly by the institutional investor, the institutional investor shall send the trade confirmation of acceptance or rejection of the contract note to the broker by using the IFN 598 messaging format. The custodian shall also send the confirmation of acceptance or rejection of such contract note to the broker using the messaging standard IFN 548.

4.4.1.3. In case the contract note is processed by the custodian on behalf of the institutional investor, the custodian shall send the confirmation of acceptance or rejection of the contract note to the broker by using the IFN 548 messaging format.

4.4.1.4. The institutional investor shall send settlement instructions to its custodian in IFN 540 to IFN 543 messaging formats to the custodian for the following trade types:

---

<sup>16</sup> Ref.No. DNPD/Cir-25/04 dated June 10, 2004

- 4.4.1.4.1. IFN 540: settlement instruction for a clearing house buy trade
  - 4.4.1.4.2. IFN 541: settlement instruction for a delivery-v/s-payment (DVP) buy trade
  - 4.4.1.4.3. IFN 542: settlement instruction for a clearing house sell trade
  - 4.4.1.4.4. IFN 543: settlement instruction for a delivery-v/s-payment (DVP) sell trade
  - 4.4.1.5. The custodian shall confirm/ reject the execution of the settlement instructions to the institutional investor in IFN 544 to IFN 547 messaging formats in the following manner:
    - 4.4.1.5.1. IFN 544: confirmation / rejection of an instruction received in messaging format IFN 540
    - 4.4.1.5.2. IFN 545: confirmation / rejection of an instruction received in messaging format IFN 541
    - 4.4.1.5.3. IFN 546: confirmation / rejection of an instruction received in messaging format IFN 542
    - 4.4.1.5.4. IFN 547: confirmation / rejection of an instruction received in messaging format IFN 543
  - 4.4.1.6. It is clarified that if a message (for the activities mentioned above) is sent using the STP centralised hub framework from one user to another user, then the confirmation / rejection for such a message shall also be sent using the STP centralised hub framework.
- 4.4.2. Please refer to the format for the electronic contract note prescribed at Annexure III. After deliberation with the STP service providers and the market participants, the following changes have been incorporated to the existing messaging format (IFN 515):
- 4.4.2.1. The mandatory requirement of mentioning the relevant bye-laws / rules / regulations of the exchange subject to which the said contract note is being issued on each contract note stands modified in the following manner:
    - 4.4.2.1.1. The requirement is not mandatory but optional.
    - 4.4.2.1.2. The broker shall ensure that the relevant bye-laws / rules / regulations of the exchange subject to which the contract note is being issued, is mentioned in the broker-client agreement and the tripartite agreement between the broker-AP-client agreement (if applicable).

- 4.4.2.1.3. The existing field for the above provision shall not be deleted and may be used as a free text field for one constituent to communicate remarks (if any) to another constituent.
- 4.4.2.2. The clause of 'payment of consolidated stamp duty' for each contract note shall be mentioned in the broker-client agreement and the tripartite agreement between the broker-AP-client agreement (if applicable). The said clause may be stated in the free text field (as mentioned in point 2 (a) (iii) above) of each contract note.
- 4.4.2.3. In the field "market type" (field 70E) a category of 'TT' i.e. trade for trade and 'OT' i.e. Others shall be added to represent the supplementary categories of market types.
- 4.4.2.4. The order time was prescribed as a mandatory field in the contract note. The order time shall now be included in the optional fields.
- 4.4.2.5. There are certain securities which are not de-materalised and hence do not have an ISIN code. For such securities (where ISIN number is not available) the STP users would be required to input the security code given by the exchange in the ISIN number field. In case the number length of the exchange scrip code is shorter than the prescribed field length of 12 characters, the code shall be prefixed with zeros.
- 4.4.2.6. In order to maintain a complete audit trail, it is clarified that in case an electronic contract note is rejected, the custodian (in messaging format IFN 548) or the fund manager (in messaging format IFN 598) shall be required to send a rejection message to the broker. Only on receipt of the rejection message, the broker shall cancel the rejected contract note and issue a fresh contract note bearing a new number.
- 4.4.2.7. In order to bring in standardisation in the input of the identification codes in the prescribed messaging standards, it is clarified that the following codes shall be used by the various entities:
- 4.4.2.7.1. **Brokers:** SEBI registration number
  - 4.4.2.7.2. **Mutual Funds and schemes of Mutual Funds:** SEBI registration number for Mutual Funds and Unique client code issued by the exchanges for schemes
  - 4.4.2.7.3. **FPIs:** SEBI registration number for the Foreign Portfolio Investors ("FPIs")
  - 4.4.2.7.4. **Custodians:** SEBI registration number
  - 4.4.2.7.5. **STP service providers and STP centralised hub:** PAN
  - 4.4.2.7.6. **Depositories and exchanges / clearing house / clearing corporation:** PAN
  - 4.4.2.7.7. **Other Institutional Investors like financial institutions, banks etc.:** Unique client code issued by the exchanges

4.4.2.8. All market participants shall issue the electronic contract note for institutional trades in the modified format.

4.4.3. After consultation with the market participants and confirming their preparedness, it has been decided to make the messaging formats for IFN 540, IFN 541, IFN 542, IFN 543, IFN 544, IFN 545, IFN 546, IFN 547, IFN 548 and IFN 598 (in addition to IFN 515) mandatory for all institutional trades.

4.4.4. It is reiterated that the STP system shall be initially mandatory for all institutional trades in the equity segment.

4.4.5. The standard terms of contract as are required to be mentioned in the Contract Notes as per the Bye-laws and Regulations of exchanges, which are not contained in electronic contract notes, shall be incorporated in the Client Broker Agreement or where applicable, the Tripartite Agreement between the stock broker, AP and the client. The stamp duty in respect of the electronic contract notes shall be paid by the broker.

#### 4.5. Clarification<sup>17</sup>

4.5.1. Descriptors as stated above shall mean the following:

- 4.5.1.1. IFN 540: settlement instruction for a buy trade free of payment
- 4.5.1.2. IFN 541: settlement instruction for a buy trade against payment
- 4.5.1.3. IFN 542: settlement instruction for a sell trade free of payment
- 4.5.1.4. IFN 543: settlement instruction for a sell trade against payment
- 4.5.1.5. IFN 544: confirmation of a settlement instruction for a buy trade free of payment (response to IFN 540)
- 4.5.1.6. IFN 545: confirmation of a settlement instruction for a buy trade against payment (response to IFN 541)
- 4.5.1.7. IFN 546: confirmation of a settlement instruction for a sell trade free of payment (response to IFN 542).
- 4.5.1.8. IFN 547: confirmation of a settlement instruction for a sell trade against payment (response to IFN 543).

4.5.2. It is also clarified that in the IFN 515 message, if trade is intended to be settled by the custodian with the Clearing Corporation (by accepting the settlement obligation), then it shall be termed as "FREE" and if the trade is intended to be

---

<sup>17</sup> Ref. No. DNP/14785/04 dated July 08, 2004

settled by the broker with the Clearing Corporation then it shall be termed as "APMT" (meaning against payment) in the tag 22h of the IFN 515 message.

#### 4.6. Modifications in the prescribed messaging formats<sup>18</sup>

In order to integrate the STT in the STP system, it would be necessary to provide for necessary fields in the appropriate messaging standards. After deliberation with the STP centralised hub and the STP service providers, it has been decided to make the following modifications in the prescribed messaging formats:

##### 4.6.1. Message Types that shall be modified are **IFN515, IFN540, IFN541, IFN542 and IFN543**

A Qualifier shall be used to identify Securities Transaction Tax Amount: "COUN", Country, National Federal Tax.

##### 4.6.2. The change in the ISO Structure for the impacted message types shall be as follows:

M	16R		AMT	Start of block	
M	19A	Amount	:4!c//3!a11d	To identify the Securities Transaction Tax Amount	Format: (Qualifier) //(Currency Code) (Amount) For: Securities Transaction tax Amount Qualifier: "COUN" (4 Upper case Characters) Narrative: "INR" (3 Upper Letters) Amount: Up to 10 digits (only Integer value allowed) followed by a comma (used as decimal sign) . Comma is mandatory. Amount can be zero or greater than zero.
M	16S		AMT	End of block	

<sup>18</sup> Ref. No. DNP/28/04 dated September 28, 2004

- 4.6.3. Securities Transaction Tax Block shall be placed before the Settlement Amount Block in the stated Message Types. (IFN515, IFN540, IFN541, IFN542 and IFN543)
- 4.6.4. Securities Transaction Tax block will be **mandatory amount block** in IFN515 and **optional amount block** in IFN540, IFN541, IFN542 and IFN543.
- 4.6.5. If the Contract Note (issued by means of IFN 515) is rejected on the basis of Securities Transaction Tax amount, then the reason for the rejection shall be specified in the "Tag70D Narrative" field and "Tag 24B Reason" specified should be "NARR".

## 5. TRADING TERMINALS

### 5.1. Testing of software used in or related to Trading and Risk Management<sup>19</sup>

#### 5.1.1. Meaning

For the purpose of this section, 'Software' shall mean electronic systems or applications used by stock brokers / trading members for connecting to the stock exchanges and for the purposes of trading and real-time risk management, including software used for Internet Based Trading ("IBT"), Direct Market Access ("DMA"), Securities Trading using Wireless Technology ("STWT"), Smart Order Routing ("SOR"), Algorithmic Trading ("AT"), etc.

#### 5.1.2. Testing of Software

In addition to the testing and approval requirements specified through various circulars issued by SEBI on IBT, DMA, STWT, SOR and AT, 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:

5.1.2.1. **Testing in a simulated test environment:** Stock exchanges shall provide suitable facilities to market participants / software vendors to test new software or existing software that have undergone change. Subjecting the new software or existing software that have undergone change to such testing facility shall be mandatory for market participants, before putting it in use.

#### 5.1.2.2. Mock testing

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

---

<sup>19</sup> Circular No. CIR/MRD/DP/24/2013 dated August 19, 2013 and CIR/MRD/DP/06/2014 dated February 07, 2014

- 5.1.2.2.2. Stock exchanges shall mandate a minimum time period for such testing in the mock trading sessions.
- 5.1.2.2.3. In order to improve the efficacy of the mock trading sessions, all stock brokers / trading members shall ensure that all user-ids approved for Algo trading, irrespective of the algorithm having undergone change or not, shall participate in the mock trading sessions.
- 5.1.2.2.4. User Acceptance Test (“UAT”): The stock broker/ trading member shall undertake UAT of the software to satisfy itself that the newly developed/ modified software meets its requirements.
- 5.1.2.2.5. 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<sup>20</sup>:
- 5.1.2.2.5.1. The test environment shall be made available to all the members.
  - 5.1.2.2.5.2. The test environment shall be made available for at least two hours after market hours and at least on two trading days in a week.
  - 5.1.2.2.5.3. For the purpose of testing, Stock Exchange shall make available data from at least one trading day in all segments and the same shall not be older than one month from the day of the testing environment.
  - 5.1.2.2.5.4. All trading members (excluding those who use only Exchange provided front end and/or ASP services) having approved Algorithms available with the member, 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.
  - 5.1.2.2.5.5. Exchange shall provide a daily log, including Algos used, of members’ participation in Simulated Environment to all participating members. The Exchange shall provide summary report of such activity to SEBI.
- 5.1.2.3. With respect to testing of software related to (a) fixes to bugs in the software, (b) changes undertaken to the stock brokers’ software/ systems pursuant to a change to any stock exchange's trading system, and (c) software purchased from a software vendor that has already been tested in the mock environment by certain number of stock brokers, stock exchanges may

---

<sup>20</sup> Circular No. SEBI/HO/MRD1/DSAP/CIR/P/2020/234 dated November 24, 2020

prescribe a faster approval process to make the process of approval expeditious.

- 5.1.3. Stock brokers / trading members shall also engage system auditor(s) to examine reports of mock tests and UAT in order to certify that the tests were satisfactorily undertaken.
- 5.1.4. Stock exchanges shall monitor compliance of stock brokers / trading members, who use trading algorithm, with regard to the requirement of participation in mock trading session as mandated with this circular. In cases where stock exchanges find that the stock broker / trading member has failed to participate in such mock trading sessions, stock exchange shall call for reasons and if found unsatisfactory, shall suspend the proprietary trading rights of the stock broker/ trading member for a minimum period of one trading day.
- 5.1.5. Stock exchanges shall also ensure that the system auditors examine the compliance of stock broker / trading member, who use trading algorithms, with regard to the requirement of participation in mock trading session, as mandated with this circular, and provide suitable comments in the periodic system audit report. In cases where the system audit report indicate that the stock broker / trading member has failed to participate in such mock trading sessions, stock exchange shall call for reasons from the stock broker/trading member and if found unsatisfactory, shall suspend the proprietary trading rights of the stock broker / trading member for a minimum period of one trading day.
- 5.1.6. For pre-approval / periodic system audit of Computer-to-Computer Link (“CTCL”) or Intermediate Messaging Layer (“IML”), IBT, DMA, STWT, SOR and AT, stock brokers / trading members shall engage a system auditor with any of the certifications as specified in Clause 7.1.4 of this Chapter of Master Circular for Stock Exchanges and Clearing Corporations. While finalizing the system auditor, stock brokers / trading members shall ensure the system auditor does not have any conflict of interest with the stock broker and the directors/promoters of the system auditor are not directly or indirectly related to the current directors or promoters of stock broker / trading member.

#### **5.1.7. Approval of Software of stock broker / trading member**

- 5.1.7.1. Stock brokers / trading members shall seek approval of the respective stock exchanges for deployment of the software in the securities market by submitting necessary details required by stock exchange including details of software, tests undertaken and certificate / report provided by the system

auditor. Stock exchange may seek additional details as deemed necessary for evaluating the application of the stock broker / trading member.

- 5.1.7.2. Stock exchanges shall grant approval or reject the application of the stock broker as the case may be, and communicate the decision to the stock broker / trading member within fifteen working days from the date of receipt of completed application (or within any other such time period specified vide SEBI circulars on DMA, IBT, STWT, SOR, AT, etc.). In case of rejection of the application, the stock exchange shall also communicate reasons of rejection to the stock broker / trading member within such time period.
- 5.1.7.3. Before granting approval to use software in securities market, stock exchange shall ensure that the requirements specified by SEBI / stock exchange with regard to software are met by the stock broker / trading member.
- 5.1.7.4. Stock exchanges may suitably schedule the requirements of mock testing, certification of test reports by system auditor(s) and the software approval process, so as to facilitate a speedy approval and a smooth transition of the stock brokers to the new / upgraded software.

5.1.8. In order to ensure that stock brokers are not using software without requisite approval of the stock exchanges, stock exchanges are advised to put in place suitable mechanism to prevent any unauthorized change to the approved software.

#### **5.1.9. Undertaking to be provided by stock brokers / trading members**

- 5.1.9.1. Stock brokers / trading members shall submit an undertaking to the respective stock exchanges stating the following at the minimum:
- 5.1.9.2. M/s (name of the stock broker / trading member) will take all necessary steps to ensure that every new software and any change thereupon to the trading and/or risk management functionalities of the software will be tested as per the framework prescribed by SEBI / stock exchange before deployment of such new / modified software in securities market.
- 5.1.9.3. M/s (name of the stock broker / trading member) will ensure that approval of the stock exchange is sought for all new / modified software and will comply with various requirements specified by SEBI or the stock exchange from time to time with regard to usage, testing and audit of the software.
- 5.1.9.3.1. The absolute liability arising from failure to comply with the above provisions shall lie entirely with M/s (name of the stock broker / trading member).

- 5.1.9.4. Stock exchanges may include additional clauses as deemed necessary in the undertaking.
- 5.1.10. Sharing of Application Programming Interface (API) specifications by the stock exchange with stock brokers / trading members
- 5.1.10.1. 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. Stock brokers / trading members and software vendors require relevant API specifications to facilitate interaction of the developed software with the systems of the stock exchanges.
- 5.1.10.2. Technical Advisory Committee (TAC) had engaged with stock exchanges, software vendors and stock brokers / trading members to review the framework of sharing of APIs by stock exchanges.
- 5.1.10.3. Based on the recommendations of the committee, it is decided that stock exchanges shall provide relevant API specifications to all stock brokers / trading members and software vendors who are desirous of developing software for the securities market, after establishing their respective credentials.
- 5.1.10.4. In case of refusal to share APIs, stock exchanges shall provide reasons in writing to the desirous stock brokers / trading members or software vendors within a period of fifteen working days from the date of receipt of such request for sharing of API.
- 5.1.10.5. Further, stock exchanges shall not selectively release updates / modifications, if any, of the existing API specifications to few stock brokers / trading members or software vendors ahead of others and shall provide such updated / modified API specifications to all stock brokers / trading members and software vendors with whom the earlier API specifications were shared.
- 5.1.11. **Penalty on malfunction of software used by stock broker/trading member:**

Stock exchanges shall examine the cases of malfunctioning of software used by stock brokers / trading members and apply deterrent penalties in form of fines or suspension to the stock broker/trading member whose software malfunctioned. In addition, stock brokers/trading members shall implement

various mechanisms including the following to minimize their losses in the event of software malfunction:

- 5.1.11.1. include suitable clauses in their agreement with the software vendors to define liabilities of software vendor and stock broker / trading member in case of software malfunction, and / or,
- 5.1.11.2. consider taking suitable insurance cover to meet probable losses in case of software malfunction.
- 5.1.12. With regard to changes / updates to stock broker's trading software that intend to modify the 'look and feel' and do not affect the risk management system of the stock broker or the connectivity of the trading software with stock exchange's trading system, it is clarified that mock testing and consequent system audit may not be insisted upon by the stock exchanges.
- 5.1.13. Stock exchanges shall direct their stock brokers 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 stock brokers' trading system.

## 5.2. Standing Committee<sup>21</sup>

5.2.1. A standing Committee shall be set up by each Stock Exchange to investigate the problem of computerised trading system, such as hanging/ slowdown/ breakdown. The Standing Committee shall introduce an outside computer expert. The Committee will submit a report to the Governing Board of the Stock Exchange and the Governing Board shall deliberate on the report and take suitable action/remedial measure.

5.2.2. The standing committee is required to be set up with the objective to investigate problems of computerised trading system, such as, **hanging/ slowdown/ breakdown**. With the view to ensure implementation/ compliance, the exchanges are advised as under:

- 5.2.2.1. All instances of hanging / slowdown / breakdown and any other problem in the computerized trading system, even if the disruption is less than five minutes, should be reported to the Committee for its consideration.
- 5.2.2.2. The Committee, upon examination of the issue/s shall submit a report to the Governing Board of the Stock Exchange.

---

<sup>21</sup> Circular No. MRD/DoP/SE/Cir- 14/2006 dated September 28, 2006

- 5.2.2.3. The Governing Board of the Stock Exchange shall deliberate on the aforesaid report and take suitable action / remedial measure.
- 5.2.2.4. Further, in case of stoppage beyond five minutes the exchange should also explain and report to SEBI about the incident as well as the remedial measures taken. The Stock Exchange shall also issue a press release in this regard for greater transparency and in the interest of investors.

### 5.3. **Expansion of trading terminals of the Exchange<sup>22</sup>**

The stock exchanges are allowed to set-up terminals at any place in the country, subject to the following conditions:

- 5.3.1. The Exchange shall ensure that there is adequate monitoring and surveillance mechanism for such outstation terminals in order to oversee the trades;
- 5.3.2. All such trades shall be subject to usual margin, capital adequacy and inter-day trading limits fixed for the brokers by the Exchange;
- 5.3.3. The Exchange shall ensure that investors eventually do not pay the brokerage on such trades exceeding the maximum brokerage permitted as per the rules of the Exchanges; and
- 5.3.4. The Exchange shall introduce the system of guaranteeing trades or set up a Clearing Corporation.

### 5.4. **Broad Guidelines for opening Trading Terminals abroad<sup>23</sup>**

The guidelines relating to eligibility norms, RBI permission, Permission from Foreign Regulatory Authority, Operation of terminals, Contract note, Settlement Procedure, Surveillance and Monitoring, Jurisdiction etc. for opening trading terminals abroad are provided below.

With the rapid expansion of the Indian capital market it was felt that a facility should be provided whereby an eligible overseas investor can place an order on a real-time basis, rather than telephonically. The Stock Exchanges/ Members shall follow the following guidelines for opening and maintaining the trading terminals abroad:

---

<sup>22</sup> Circular No. SMD/POLICY CIR-33/99 dated October 15, 1999

<sup>23</sup> Circular No. SMDRP/POLICY/TTA-14072/CIR-23/99 dated July 12, 1999

#### **5.4.1. Eligibility Criteria**

Such trading terminals shall be opened only by the Stock Brokers of the stock exchanges registered with SEBI and opening of terminals through APs shall not be permitted. These terminals shall be opened by the members only after obtaining permission from the respective stock exchanges.

#### **5.4.2. RBI Permission**

Such terminals abroad would be opened subject to the guidelines laid down by the RBI from time to time.

#### **5.4.3. Permission by the Foreign Regulatory Authorities**

The installation of such trading terminals shall be subject to the prior permission of the concerned regulatory authorities of the respective foreign countries, wherever required.

#### **5.4.4. Operation of the terminals**

Any investor abroad who is permitted to invest in India i.e. NRIs/OCBs/FPIs/PIOs shall be able to place orders on the trading terminal of the Exchange available at the office of the Indian broker maintained abroad. The order fed on the live terminal shall be executed on the computer of the Exchange in India. The service to the clients shall be provided by the broker's overseas office and its local office. These terminals shall include any of other options that the respective exchange may provide for connecting its trading terminal abroad to its trading system in India.

#### **5.4.5. Contract Note**

The contract note in favour of the client abroad shall be issued in India, however the same could be printed in the broker's office abroad and shall be subject to the jurisdiction of the respective stock exchanges.

#### 5.4.6. Capital Adequacy, Margins System & Brokerage

- 5.4.6.1. All such trades would be subject to usual margins, capital adequacy and intra-day trading limits and such other requirements fixed for the brokers by the Exchange.
- 5.4.6.2. The respective stock exchange shall ensure that investors do not pay the brokerage on such trades exceeding the maximum brokerage permitted as per the rules, regulations and bye-laws of the exchange.
- 5.4.6.3. No Negotiated Deals shall be permitted through these terminals and only screen based order matching system shall be available on these terminals.

#### 5.4.7. Settlement Procedure

All trades shall be settled in India in dematerialized form only. Clients with status of FPIs shall settle the trade through their registered custodian/designated bank. Clients with the status of NRIs/PIOs/OCBs shall settle the trade through a designated bank. Such a designated bank shall be responsible for repatriation of funds.

#### 5.4.8. Monitoring & Surveillance

The respective stock exchange shall ensure that there is adequate monitoring and surveillance mechanism for such overseas terminals in order to oversee trades.

#### 5.4.9. Grievance Redressal Mechanism

- 5.4.9.1. The investors' grievance for such cases shall be resolved by the respective Indian Stock Exchange through the existing arbitration mechanism.
- 5.4.9.2. The concerned Stock Exchange shall ensure that their members have the adequate arrangements for resolving the investors grievances and timely settlement of arbitration cases arising out of trades which are executed on these terminals.

#### 5.4.10. Jurisdiction

The agreement between the trading member and constituent should, inter alia, state that, all trades, transactions and contracts are subject to the Rules, Bye Laws and Regulations of the Exchange and shall be deemed to be and shall take effect as wholly made, entered into and to be performed in the city of \_\_\_\_\_, India

and the parties to such trade shall be deemed to have submitted to the jurisdiction of the Courts in \_\_\_\_\_, India for the purpose of giving effect to the provisions of the Rules, Bye Laws and Regulations of the Exchange.

#### 5.5. Safeguards to avoid trading disruption in case of failure of software vendor<sup>24</sup>

Software vendors who provide software to market participants and market infrastructure institutions for the purpose of trading, risk management, clearing and settlement play a crucial role in the securities market. Any inability on the part of such software vendors to provide software or related services in timely and continuous manner may create a situation of stress in the securities market. In view of the above, stock exchanges may advise the stock brokers to take the following measures:

- 5.5.1. Explore the possibility of establishing a 'software escrow arrangement' with their existing software vendors.
- 5.5.2. In case of large stock brokers, consider reducing dependence on a single software vendor for trading and risk management systems, by engaging more than one software vendor.
- 5.5.3. Consider including the following in their contracts with the software vendors:
  - 5.5.3.1. access to documents related to design and development specifications in the event software vendor fails to provide continuous and timely services to the stock broker;
  - 5.5.3.2. development of expertise at the end of the stock broker through appropriate training with regard to software usage and maintenance;
  - 5.5.3.3. appropriate penalty clauses for cases of disruptions to the trading system of the stock broker on account of (a) software vendor failing to provide continuous and timely services to the stock broker or (b) glitches to the software provided by the software vendor;
  - 5.5.3.4. obligation on the part of the software vendor to cooperate in case of audit of software including forensic audit, if required.

---

<sup>24</sup> Circular No. CIR/MRD/DP/07/2014 dated February 11, 2014



## 6. SMART ORDER ROUTING

### 6.1. Introduction of Smart Order Routing<sup>25</sup>

- 6.1.1. SEBI has received proposal from the stock exchanges and market participants for introducing Smart Order Routing ("SOR") which allows the brokers trading engines to systematically choose the execution destination based on factors viz. price, costs, speed, likelihood of execution and settlement, size, nature or any other consideration relevant to the execution of the order.
- 6.1.2. Upon examination of the proposal, feedback of the stock exchanges and based on the recommendations of the Technical Advisory Committee, it has been decided to permit SOR in Indian Securities Market.
- 6.1.3. Stock Exchanges are advised to ensure the following conditions with regard to SOR:
- 6.1.3.1. Stock broker interested to offer SOR facility shall apply to the respective stock exchanges.
  - 6.1.3.2. Stock broker shall submit a third party system audit of its SOR system and software. Stock exchanges shall disseminate to its stock brokers a list of approved system auditors (CISA or equivalent) qualified to undertake such system audits.
  - 6.1.3.3. Stock broker shall provide the following to the respective stock exchanges:
    - 6.1.3.3.1. An undertaking to the respective stock exchanges that SOR shall route orders in a neutral manner.
    - 6.1.3.3.2. Provide the features of the SOR to stock exchange.
  - 6.1.3.4. Stock exchange shall communicate its decision to the broker within 30 calendar days from the date of receipt of complete application by the stock exchange. Stock exchange shall not consider testing and demonstration of the SOR system/software as a criterion for declaring the application of the broker as 'complete'. Further, testing and demonstration of SOR system/software, if required, shall be suitably scheduled within the aforesaid period of 30 calendar days.

---

<sup>25</sup> Circular No. CIR/MRD/DP/26/2010 dated August 27, 2010



In case of rejection of the application on smart order routing of a stock broker, the stock exchange shall communicate such reasons of rejections to the stock broker. Further, the decision of the stock exchange on the SOR application of the stock broker and reasons for rejection of the SOR application shall also be communicated to all the other stock exchanges where the broker's SOR facility intends to route orders.<sup>26</sup>

- 6.1.3.5. Stock exchange shall ensure that brokers adhere to the best execution policy while using SOR.
- 6.1.3.6. SOR facility shall be provided to all class of investors.
- 6.1.3.7. Stock Broker shall communicate to all clients the features, possible risks, rights, responsibilities and liabilities associated with the smart order routing facility. The client desirous of availing such facility shall do so by entering into a broker-client agreement, as applicable. For the existing clients, the same shall be implemented through an addendum to the existing broker-client agreement, as applicable.<sup>27</sup>
- 6.1.3.8. Stock broker shall maintain logs of all activities to facilitate audit trail. Broker shall maintain record of orders, trades and data points for the basis of decision.
- 6.1.3.9. In case the client has availed Smart Order Routing facility and does not want to use the same for a particular order, the same shall be well documented by the stock broker.
- 6.1.3.10. System audit of the SOR systems and software shall be periodically carried out by the brokers as may be specified by the exchange and certificate in this regard shall be submitted to the exchange.
- 6.1.3.11. Stock exchange shall ensure that SOR is not used to place orders at venues other than the recognised stock exchanges.
- 6.1.3.12. The stock broker shall carry out appropriate validation of all risk parameters before the orders are placed in the SOR system.
- 6.1.3.13. Stock exchange shall provide unique identification number for the orders placed through SOR system. Further, stock exchanges shall maintain data on SOR orders and trades.
- 6.1.3.14. Stock exchange shall have necessary surveillance mechanism in place to monitor trading done through SOR.
- 6.1.3.15. Stock broker shall ensure that alternative mode of trading system is available in case of failure of SOR facility.

---

<sup>26</sup> Circular No. CIR/MRD/DP/ 36 /2010 dated December 09, 2010

<sup>27</sup> Circular No. CIR/MRD/DP/ 36 /2010 dated December 09, 2010



- 6.1.3.16. Stock exchange shall ensure that within a period of three months from implementation of SOR, a system is put in place to time stamp market data feed that is disseminated to the market, if the same is not already available.
- 6.1.3.17. Stock exchange shall strengthen investor grievance cell in order to address complaints, if any, received with regard to SOR. Further, in case of any disputes or complaints, stock exchanges shall share necessary data as and when required in order to facilitate necessary examination.
- 6.1.3.18. Stock exchange shall synchronise their system clocks with atomic clock before the start of market.
- 6.1.3.19. The broker server routing orders placed through the SOR system to the exchange trading system shall be located in India. Stock exchange shall permit SOR approved brokers to offer SOR facility through all their servers irrespective of their location in India.<sup>28</sup>
- 6.1.3.20. All other existing obligations for the broker as per current regulations and circulars will continue.
- 6.1.3.21. Stock exchange may specify additional safeguards as they deem fit for allowing SOR facility to their brokers.
- 6.1.3.22. Stock exchange shall permit smart order routing for all orders, without restricting to any specific type of order. The choice on order types shall be left to the client.<sup>29</sup>
- 6.1.3.23. If stock exchange desires to advise its brokers to seek re-approval, it may do so only in case of <sup>30</sup>
- 6.1.3.23.1. Inclusion of a new stock exchange for offering SOR facility; and/or,
- 6.1.3.23.2. Material changes in the software/system of the SOR facility.

---

<sup>28</sup> Circular No. CIR/MRD/DP/ 36 /2010 dated December 09, 2010

<sup>29</sup> Circular No. CIR/MRD/DP/ 36 /2010 dated December 09, 2010

<sup>30</sup> Circular No. CIR/MRD/DP/ 36 /2010 dated December 09, 2010



## 7. ALGORITHMIC TRADING

### 7.1. Broad Guidelines on Algorithmic Trading<sup>31</sup>

#### Definition

**7.1.1. Algorithmic Trading:** Any order that is generated using automated execution logic shall be known as algorithmic trading.

#### Guidelines to the stock exchanges and the stock brokers

7.1.2. Stock exchanges shall ensure the following while permitting algorithmic trading:

- 7.1.2.1. The stock exchange shall have arrangements, procedures and system capability to manage the load on their systems in such a manner so as to achieve consistent response time to all stock brokers. The stock exchange shall continuously study the performance of its systems and, if necessary, undertake system upgradation, including periodic upgradation of its surveillance system, in order to keep pace with the speed of trade and volume of data that may arise through algorithmic trading.
- 7.1.2.2. In order to ensure maintenance of orderly trading in the market, stock exchange shall put in place effective economic disincentives with regard to high daily order-to-trade ratio of algo orders of the stock broker. Further, the stock exchange shall put in place monitoring systems to identify and initiate measures to impede any possible instances of order flooding by algos.
- 7.1.2.3. In order to discourage repetitive instances of high daily order-to-trade ratio, stock exchanges shall impose an additional penalty in form of suspension of proprietary trading right of the stock broker for the first trading hour on the next trading day in case a stock broker is penalized for maintaining high daily order-to-trade ratio, provided penalty was imposed on the stock broker on more than ten occasions in the previous thirty trading days.
- 7.1.2.4. The stock exchange shall ensure that all algorithmic orders are necessarily routed through broker servers located in India and the stock exchange has appropriate risk controls mechanism to address the risk emanating from

---

<sup>31</sup> Circular No. CIR/MRD/DP/09/2012 dated March 30, 2012 and Circular No. CIR/MRD/DP/16/2013 dated May 21, 2013



algorithmic orders and trades. The minimum order-level risk controls shall include the following:

- 7.1.2.4.1. Price check - The price quoted by the order shall not violate the price bands defined by the exchange for the security. For securities that do not have price bands, *dummy filters* shall be brought into effective use to serve as an early warning system to detect sudden surge in prices.
- 7.1.2.4.2. Quantity Limit check - The quantity quoted in the order shall not violate the maximum permissible quantity per order as defined by the exchange for the security.
- 7.1.2.5. In the interest of orderly trading and market integrity, the stock exchange shall put in place a system to identify dysfunctional algos (i.e. algos leading to loop or runaway situation) and take suitable measures, including advising the member, to shut down such algos and remove any outstanding orders in the system that have emanated from such dysfunctional algos. Further, in exigency, the stock exchange should be in a position to shut down the broker's terminal.
- 7.1.2.6. Terminals of the stock broker that are disabled upon exhaustion of collaterals shall be enabled manually by the stock exchange in accordance with its risk management procedures.
- 7.1.2.7. The stock exchange may seek details of trading strategies used by the algo for such purposes viz. inquiry, surveillance, investigation, etc.
- 7.1.2.8. In order to strengthen the surveillance mechanism related to algorithmic trading and prevent market manipulation, stock exchanges are directed to take necessary steps to ensure effective monitoring and surveillance of orders and trades resulting from trading algorithms. Stock exchanges shall periodically review their surveillance arrangements in order to better detect and investigate market manipulation and market disruptions.
- 7.1.2.9. The stock exchange shall submit a report on algorithmic trading on the stock exchange inter-alia incorporating turnover details of algorithmic trading, algorithmic trading as percentage of total trading, number of stock brokers / clients using algorithmic trading, action taken in respect of dysfunctional algos, status of grievances, if any, received and processed, etc.



7.1.2.10. The stock exchange shall synchronize its system clock with the atomic clock before the start of market such that its clock has precision of atleast one microsecond and accuracy of atleast +/- one millisecond.

7.1.3. Stock exchange shall ensure that the stock broker shall provide the facility of algorithmic trading only upon the prior permission of the stock exchange. Stock exchange shall subject the systems of the stock broker to initial conformance tests to ensure that the checks mentioned below are in place and that the stock broker's system facilitate orderly trading and integrity of the securities market. Further, the stock exchange shall suitably schedule such conformance tests and thereafter, convey the outcome of the test to the stock broker.

For stock brokers already providing algo trading, the stock exchange shall ensure that the risk controls specified in this circular are implemented by the stock broker.

7.1.4. The stock brokers that provide the facility of algorithmic trading shall subject their algorithmic trading system to a system audit every six months in order to ensure that the requirements prescribed by SEBI / stock exchanges with regard to algorithmic trading are effectively implemented. Such system audit of algorithmic trading system shall be undertaken by a system auditor who possess any of the following certifications:

- 7.1.4.1. CISA (Certified Information System Auditors) from ISACA;
- 7.1.4.2. DISA (Post Qualification Certification in Information Systems Audit) from Institute of Chartered Accountants of India (ICAI);
- 7.1.4.3. CISM (Certified Information Securities Manager) from ISACA;
- 7.1.4.4. CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium, commonly known as (ISC)<sup>2</sup>.

7.1.5. Deficiencies or issues identified during the process of system audit of trading algorithm / software shall be reported by the stock broker to the stock exchange immediately on completion of the system audit. Further, the stock broker shall take immediate corrective actions to rectify such deficiencies / issues.

7.1.6. In case of serious deficiencies / issues or failure of the stock broker to take satisfactory corrective action, the stock exchange shall not allow the stock broker



to use the trading software till deficiencies / issues with the trading software are rectified and a satisfactory system audit report is submitted to the stock exchange. Stock exchanges may also consider imposing suitable penalties in case of failure of the stock broker to take satisfactory corrective action to its system within the time-period specified by the stock exchanges. Further, the stock exchange shall subject the stock broker systems to more frequent system audits, if required.

7.1.7. The stock broker, desirous of placing orders generated using algos, shall satisfy the stock exchange with regard to the implementation of the following minimum levels of risk controls at its end -

- 7.1.7.1. *Price check* - Algo orders shall not be released in breach of the price bands defined by the exchange for the security.
- 7.1.7.2. *Quantity check* - Algo orders shall not be released in breach of the quantity limit as defined by the exchange for the security.
- 7.1.7.3. *Order Value check* - Algo orders shall not be released in breach of the 'value per order' as defined by the stock exchanges.
- 7.1.7.4. *Cumulative Open Order Value check* - The individual client level cumulative open order value check, may be prescribed by the broker for the clients. Cumulative Open Order Value for a client is the total value of its unexecuted orders released from the stock broker system.
- 7.1.7.5. *Automated Execution check* - An algo shall account for all executed, un-executed and unconfirmed orders, placed by it before releasing further order(s). Further, the algo system shall have pre-defined parameters for an automatic stoppage in the event of algo execution leading to a loop or a runaway situation.
- 7.1.7.6. All algorithmic orders are tagged with a unique identifier provided by the stock exchange in order to establish audit trail.

7.1.8. The other risk management checks already put in place by the exchange shall continue and the exchange may re-evaluate such checks if deemed necessary in view of algo trading.

7.1.9. The stock broker, desirous of placing orders generated using algos, shall submit to the respective stock exchange an undertaking that -

- 7.1.9.1. The stock broker has proper procedures, systems and technical capability to carry out trading through the use of algorithms.



- 7.1.9.2. The stock broker has procedures and arrangements to safeguard algorithms from misuse or unauthorized access.
  - 7.1.9.3. The stock broker has real-time monitoring systems to identify algorithms that may not behave as expected. Stock broker shall keep stock exchange informed of such incidents immediately.
  - 7.1.9.4. The stock broker shall maintain logs of all trading activities to facilitate audit trail. The stock broker shall maintain record of control parameters, orders, trades and data points emanating from trades executed through algorithm trading.
  - 7.1.9.5. The stock broker shall inform the stock exchange on any modification or change to the approved algos or systems used for algos.
- 7.1.10. The stock exchange, if required, shall seek conformance of such modified algo or systems to the requirements specified in the circular.



## 8. ANNUAL SYSTEM AUDIT

### 8.1. System and Network Audit of Market Infrastructure Institutions <sup>32</sup>

8.1.1. Market Infrastructure Institutions (“MIIs”) are required to conduct System and Network Audit as per the framework mentioned in Annexure V and Terms of Reference (“TOR”) mentioned in Annexure VI. MIIs are also required to maintain a list of all the relevant SEBI circulars/ directions/ advices, etc. pertaining to technology and compliance thereof, as per format placed at Annexure VII and the same shall be included under the scope of System and Network Audit.

8.1.2. MIIs are also required to submit information with regard to exceptional major Non-Compliances (NCs)/ minor NCs observed in the System and Network Audit as per format placed at Annexure VIII and are required to categorically highlight those observations/NCs/suggestions pointed out in the System and Network Audit (current and previous) which remain open.

8.1.3. The Systems and Network Audit Report including compliance with SEBI circulars/ guidelines and exceptional observation format along with compliance status of previous year observations shall be placed before the Governing Board of the MII and then the report along with the comments of the Management of the MII shall be communicated to SEBI within a month of completion of audit.

8.1.4. Further, along with the audit report, MIIs are required to submit a Joint declaration from the Managing Director(MD)/Chief Executive Officer(CEO) and Chief Technology Officer (CTO) certifying a) the security and integrity of their IT Systems b) correctness and completeness of data provided to the Auditor c) entire network architecture, connectivity (including co-lo facility) and its linkage to the trading infrastructure are in conformity with SEBI’s regulatory framework to provide fair equitable, transparent and non-discriminatory treatment to all the market participants d) internal review of Critical Systems as defined in Clause 9.1 of this Chapter of Master Circular for Stock Exchanges and Clearing Corporations was carried out during the Audit period, including the Failure Modes and Effects Analysis (FMEA).

---

<sup>32</sup> Circular No. SEBI/HO/MRD1/MRD1\_DTCS/P/CIR/2022/58 dated May 02, 2022

## 8.2. Annual System Audit of Stock Brokers<sup>33</sup>

- 8.2.1. The stock exchanges should ensure that system audit of stock brokers / trading members are conducted in accordance with the prescribed guidelines placed at Annexure IX.
- 8.2.2. Exchanges are advised to keep track of findings of system audits of all brokers on quarterly basis and ensure that all major audit findings, specifically in critical areas, are rectified / complied in a time bound manner failing which follow up inspection of such brokers may be taken up for necessary corrective steps / actions thereafter, if any.
- 8.2.3. Stock Exchange should report all major non-compliances / observations of system auditors, broker wise, on a quarterly basis to SEBI.

## 8.3. System Audit of Professional Clearing Members (PCMs)<sup>34</sup>

- 8.3.1. PCMs are required to conduct System Audit as per the framework enclosed as Annexure IXA and Terms of Reference (TOR) enclosed as Annexure IXB. PCMs are also required to maintain a list of all the relevant SEBI and CCs circulars/ directions/ advices, etc. pertaining to technology and compliance thereof, as per format enclosed as Annexure IXC and the same shall be included under the scope of System Audit.
- 8.3.2. PCMs are also required to submit information with regard to exceptional major Non-Compliances (NCs)/ minor NCs observed in the System Audit as per format enclosed as Annexure IXD and are required to categorically highlight those observations/ NCs/ suggestions pointed out in the System Audit (current and previous) which remain open.
- 8.3.3. The Systems Audit report including compliance with SEBI/CCs circulars/guidelines and exceptional observation format along with compliance status of previous year observations shall be placed before the Governing Board of the PCM and then the report along with the comments of the Management of

---

<sup>33</sup> Circular No. CIR/MRD/DMS/34/2013 dated November 06, 2013

<sup>34</sup> Circular No. SEBI/HO/MRD/TPD/P/CIR/2024/84 dated June 20, 2024



the PCM shall be communicated to CCs within one month of completion of audit.

8.3.4. All CCs are jointly advised to devise the appropriate uniform penalty structure for PCMs to ensure that system audit reports are submitted to them within defined timelines as well as audit observations are closed within defined timelines.

#### **8.4. Advisory on System and Network Audit of MIIs**

With regard to the system and network audit of the MIIs, the following needs to be ensured by the MIIs:-

8.4.1. MIIs should update the scope of system and network audit as and when any circular/letter/advisory etc. pertaining to technology is issued by SEBI.

8.4.2. MIIs should include all IT resources, which shall inter-alia includes applications, underlying hardware, and other IT infrastructure components such as load balancers, network devices, security devices etc. in the system and network audit.

8.4.3. In the system and network audit report, details such as physical locations/sites covered, engagement period of auditor, period during which audit was carried out and list of IT infrastructure/applications covered shall be specified.

8.4.4. MIIs shall cover all “Critical Systems” in system and network audit. For non-critical systems, auditors may adopt sampling methodology.

8.4.5. Sample size taken by auditor in order to ascertain the various compliances prescribed by SEBI shall be specified in the system and network audit report.

8.4.6. Technical assessments such as review of network architecture and configuration review shall be included in the system and network audit.

8.4.7. During system and network audit, evidence should be collected by inspecting physical assets, records/documents, testing of relevant systems, relevant system generated reports etc. in order to ascertain the compliance of various controls defined by SEBI.



- 8.4.8. System and network audit report shall include the point-wise compliance of areas emanating from relevant SEBI circulars/directions/advice along with any accompanying evidence.
- 8.4.9. Auditor shall certify that entire network architecture, connectivity (including co-lo facility) and its linkage to the trading infrastructure are in conformity with SEBI's regulatory framework to provide fair equitable, transparent and non-discriminatory treatment to all the market participants.
- 8.4.10. Evidence verified/checked by auditor to ascertain the compliance of particular control shall be in line with the intent/requirement of the said control mentioned in the SEBI circular pertaining to system and network audit.
- 8.4.11. All MIIs are advised to ensure the strict compliance of the said advisory and shall also bring the same to the notice of the concerned system and network auditors. The compliance of the aforesaid advisory shall be provided by MIIs along with their system and network audit report (conducted as per the applicable SEBI circular on system and network audit).



## 9. BUSINESS CONTINUITY PLAN AND DISASTER RECOVERY

### 9.1. Guidelines for Business Continuity Plan (BCP) and Disaster Recovery (DR) of Market Infrastructure Institutions (MIIs)<sup>35</sup>

9.1.1. The framework for Business Continuity Plan (BCP) and Disaster Recovery (DR) shall be as under:

- 9.1.1.1. Stock Exchanges and Clearing Corporations (which, along with Depositories, are collectively referred as Market Infrastructure Institutions – MIIs) shall have in place BCP and DRS so as to maintain data and transaction integrity.
- 9.1.1.2. For Stock Exchanges: Apart from DRS, all Stock Exchanges shall also have a Near Site (NS) to ensure near zero data loss.  
For Clearing Corporations and Depositories: Apart from DRS, all Clearing Corporations and Depositories shall also have a Near Site (NS) to ensure zero data loss
- 9.1.1.3. The DRS should preferably be set up in different seismic zones and in case due to certain reasons such as operational constraints, change of seismic zones, etc., minimum distance of 500 kilometer shall be ensured between PDC and DRS so that both DRS and PDC are not affected by the same disaster.
- 9.1.1.4. The manpower deployed at DRS shall have the same expertise as available at PDC in terms of knowledge/ awareness of various technological and procedural systems and processes relating to all operations such that DRS can function at short notice, independently. MIIs shall have sufficient number of trained staff at their DRS so as to have the capability of running live operations from DRS without involving staff of the PDC.
- 9.1.1.5. All MIIs shall constitute an Incident and Response team (IRT)/ Crisis Management Team (CMT), which shall be chaired by the Managing Director (MD) of the MII or by the Chief Technology Officer (CTO), in case of non-availability of MD. IRT/ CMT shall be responsible for the actual declaration of disaster, invoking the BCP and shifting of operations from PDC to DRS whenever required. Details of roles, responsibilities and actions to be performed by employees, IRT/ CMT and support/outsourced staff in the event of any Disaster shall be defined and documented by the MII as part of BCP-DR Policy Document.
- 9.1.1.6. The Technology Committee of the MIIs shall review the implementation of BCP-DR policy approved by the Governing board of the MII on a quarterly basis.

---

<sup>35</sup> Circular No. SEBI/HO/MRD1/DTCS/CIR/P/2021/33 dated March 22, 2021 and SEBI Circular SEBI/HO/MRD/TPD-1/P/CIR/2024/119 dated September 12, 2024



9.1.1.7. MIIs shall conduct periodic training programs to enhance the preparedness and awareness level among its employees and outsourced staff, vendors, etc. to perform as per BCP policy.

#### **9.1.2. Configuration of DRS/NS with PDC**

9.1.2.1. Hardware, system software, application environment, network and security devices and associated application environments of DRS / NS and PDC shall have one to one correspondence between them.

9.1.2.2. MIIs should develop systems that do not require configuration changes at the end of trading members/ clearing members/ depository participants for switchover from the PDC to DRS. Further, MIIs should test such switchover functionality by conducting unannounced live trading from its DRS for at least 1 day in every six months. Unannounced live trading from DRS of MIIs shall be done at a short notice of 45 minutes after 90 days from the date of this circular.

9.1.2.3. In the event of disruption of any one or more of the 'Critical Systems' (as defined below), the MII shall, within 30 minutes of the incident, declare that incident as 'Disaster' and take measures to restore operations including from DRS within 45 minutes of the declaration of 'Disaster'. Accordingly, the Recovery Time Objective(RTO)- the maximum time taken to restore operations of 'Critical Systems' from DRS after declaration of Disaster- shall be 45 minutes, to be implemented within 90 days from the date of the circular. 'Critical Systems' for an Exchange/ Clearing Corporation shall include Trading, Risk Management, Collateral Management, Clearing and Settlement and Index computation. 'Critical Systems' for a Depository shall include systems supporting settlement process and inter-depository transfer system.

9.1.2.4. MIIs shall ensure that the Recovery Point Objective (RPO) - the maximum tolerable period for which data might be lost due to a major incident - shall be near zero. Further, MIIs shall have a documented methodology for data reconciliation when resuming operations from DRS or any other site as applicable.

9.1.2.5. For Stock Exchanges: Solution architecture of PDC and DRS / NS shall ensure high availability, fault tolerance, no single point of failure, near zero data loss, and data and transaction integrity.

For Clearing Corporations and Depositories: Solution architecture of PDC and DRS / NS shall ensure high availability, fault tolerance, no single point of failure, zero data loss, and data and transaction integrity.

9.1.2.6. Any updates made at the PDC should be reflected at DRS/ NS immediately (before end of day) with head room flexibility without compromising any of the performance metrics.



- 9.1.2.7. Replication architecture, bandwidth and load consideration between the DRS / NS and PDC should be within stipulated RTO and ensure high availability, right sizing, and no single point of failure.
- 9.1.2.8. For Stock Exchanges: Synchronous replication or appropriate replication between PDC and NS shall be implemented to ensure near zero data loss. Asynchronous replication may be implemented between PDC and DRS and between NS and DRS.  
For Clearing Corporations and Depositories: Synchronous replication between PDC and NS shall be implemented to ensure zero data loss. Asynchronous replication may be implemented between PDC and DRS and between NS and DRS.
- 9.1.2.9. Adequate resources (with appropriate training and experience) should be available at all times to handle operations at PDC, NS or DRS, as the case may be, on a regular basis as well as during disasters.

### **9.1.3. DR drills/ Testing**

- 9.1.3.1. DR drills should be conducted on a quarterly basis. In case of Exchanges and Clearing Corporations, these drills should be closer to real life scenario (trading days) with minimal notice to DRS staff involved.
- 9.1.3.2. During the drills, the staff based at PDC should not be involved in supporting operations in any manner.
- 9.1.3.3. The drill should include running all operations from DRS for at least 1 full trading day.
- 9.1.3.4. Before DR drills, the timing diagrams clearly identifying resources at both ends (DRS as well as PDC) should be in place.
- 9.1.3.5. The results and observations of these drills should be documented and placed before the Governing Board of Stock Exchanges/ Clearing Corporations/ Depositories. Subsequently, the same along with the comments of the Governing Board should be forwarded to SEBI within a month of the DR drill.
- 9.1.3.6. The System Auditor while covering the BCP - DR as a part of mandated annual System Audit should check the preparedness of the MII to shift its operations from PDC to DRS unannounced and also comment on documented results and observations of DR drills.
- 9.1.3.7. 'Live' trading sessions from DR site shall be scheduled for at least two consecutive days in every six months. Such live trading sessions from the DRS shall be organized on normal working days (i.e. not on weekends / trading holidays). The Stock Exchange/ Clearing Corporation/ Depository shall ensure that staff members working at DRS have the abilities and skills to run live trading session independent of the PDC staff.



- 9.1.3.8. Stock Exchanges, Clearing Corporations and Depositories shall include a scenario of intraday shifting from PDC to DRS during the mock trading sessions in order to demonstrate its preparedness to meet RTO/RPO as stipulated above.
- 9.1.3.9. MII should undertake and document Root Cause Analysis (RCA) of their technical/ system related problems in order to identify the causes and to prevent reoccurrence of similar problems.

#### **9.1.4. BCP – DR Policy Document**

- 9.1.4.1. MIIs shall put in place a comprehensive BCP-DR policy document outlining the following:
- 9.1.4.1.1. Broad scenarios that would be defined as a Disaster for an MII (in addition to definition provided in para 4 (c) of the circular).
- 9.1.4.1.2. Standard Operating Procedure to be followed in the event of Disaster.
- 9.1.4.1.3. Escalation hierarchy within the MII to handle the Disaster.
- 9.1.4.1.4. Clear and comprehensive Communication Protocols and procedures for both internal and external communications from the time of incident till resumption of operations of the MII.
- 9.1.4.1.5. Documentation policy on record keeping pertaining to DR drills.
- 9.1.4.1.6. Scenarios demonstrating the preparedness of MIIs to handle issues in Critical Systems that may arise as a result of Disaster.
- 9.1.4.1.7. Preparedness of Depositories to handle any issue which may arise due to trading halts in Stock Exchanges.
- 9.1.4.1.8. Framework to constantly monitor health and performance of Critical Systems in normal course of business.
- 9.1.4.2. The BCP-DR policy document of MII should be approved by Governing Board of the MIIs after being vetted by Technology Committee and thereafter communicated to SEBI. The BCP-DR policy document should be periodically reviewed at least once in six months and after every occurrence of disaster.
- 9.1.4.3. In case an MII desires to lease its premise at the DRS to other entities including to its subsidiaries or entities in which it has stake, the MII should ensure that such arrangements do not compromise confidentiality, integrity, availability, targeted performance and service levels of the MII's systems at the DRS. The right of first use of all the resources at DRS including network resources should be with the MII. Further, MII should deploy necessary access controls to restrict access (including physical access) of such entities to its critical systems and networks.



9.1.5. MIIs should ensure that clauses 9.1.3.6 and 9.1.4.1.5 mentioned above are also included in the scope of System Audit.

9.1.6. MIIs are advised to collaborate in developing a standardized definition of “near zero data loss” and submit the same to SEBI after taking approval from their respective Standing Committee on Technology (SCOT).

## **9.2. Business Continuity Plan (BCP) and Disaster Recovery (DR) framework - Limited Purpose Clearing Corporation (LPCC)<sup>36</sup>**

9.2.1. The Securities Contracts (Regulation) (Stock Exchanges and Clearing Corporations) (Amendment) Regulations, 2018 has been amended to provide for a Limited Purpose Clearing Corporation (“LPCC”).

9.2.2. The LPCC has been permitted to have arrangements with any of the existing Clearing Corporations for the purposes of putting in place a BCP and DR mechanism.

9.2.3. The framework governing arrangements with existing Clearing Corporations for the purpose of BCP and DR is placed at Para 1 in Annexure X.

## **9.3. Standard Operating Procedure for handling of technical glitches by Market Infrastructure Institutions (MIIs) and payment of “Financial Disincentives” thereof<sup>37</sup>**

9.3.1. MIIs (i.e. Stock Exchanges, Clearing Corporations and Depositories) are systemically important institutions as they, inter-alia, provide infrastructure necessary for the smooth and uninterrupted functioning of the securities market.

9.3.2. With increasing dependence on technology, as the operations and functioning of MIIs are fully automated right from order entry to order matching to trade confirmation leading up to clearing and settlement of trades, the instances of technical glitches at MIIs, leading to business disruption/unavailability of services provided by MIIs, have been occurring, despite various mechanisms stipulated by SEBI such as Business Continuity Planning, Disaster Recovery policies, System Audit etc.

9.3.3. The general practice in the computing/technology industry to deal with business disruption/unavailability of services, is to work with specified downtime and for downtimes beyond such specified time, a pre-defined penalty structure is included in Service Level Agreement.

9.3.4. Considering the criticality of smooth functioning of systems of MIIs (as any disruption adversely impacts all classes of investors / market participants as well as

<sup>36</sup> Circular No. SEBI/HO/MRD2/DCAP/CIR/P/227 dated November 06, 2020

<sup>37</sup> Circular No. SEBI/HO/MRD1/DTCS/CIR/P/2021/590 dated July 05, 2021 and SEBI Circular SEBI/HO/MRD/TPD-1/P/CIR/2024/119 dated September 12, 2024



the credibility of the securities market), specifying a pre-defined threshold for downtime of systems of MIIs becomes desirable. For any downtime or unavailability of services, beyond such pre-defined time, there is a need to ensure that “Financial Disincentive” is paid by the MIIs. This will encourage MIIs to constantly monitor the performance and efficiency of their systems and upgrade/ enhance their systems etc. to avoid any possibility of technical glitches/ disruption/ disaster and restart their operations expeditiously in the event of glitch/ disruption/ disaster.

9.3.5. Accordingly, after extensive discussion with various stakeholders, it has been decided that, MIIs shall:

- 9.3.5.1. Follow the Standard Operating Procedure (SOP) for handling technical glitches as detailed at Annexure XI, and,
- 9.3.5.2. Comply with the “Financial Disincentive” structure as detailed at Annexure XII.

9.3.6. The aforesaid “Financial Disincentives”, when triggered automatically under pre-defined conditions, as detailed in Annexure XII, shall be credited to the Investor Protection Fund / Core Settlement Guarantee Fund maintained by the MII.

#### **9.4. Measures to strengthen tracking and reporting of delay in pay-in/pay-out for rolling settlement**

9.4.1. SEBI carried out review of existing SOP with regard to tracking of instances of delay in normal rolling settlement and reporting thereof to SEBI along with the joint monthly report submitted by the CCs/depositories.

9.4.2. The Competent Authority has approved the following measures subsequent to the aforesaid review to strengthen tracking of intermediate activities in rolling settlement and reporting of settlement delays. This is without prejudice to financial disincentives, if any, emanating from delay in completion of pay-in/pay-out activities.

#### **9.4.3. For tracking of intermediate activities constituting rolling settlement**

- 9.4.3.1. CCs and Depositories may put in place systems to ensure:
- 9.4.3.2. All intermediate activities that may impact rolling settlement (i.e. from trade date to settlement) are streamlined and the process flow is optimized. If there are dependencies / data shared with other CC/Depository, discussions may be done with the concerned CC / Depository with regard to optimization. Further, all intermediate activities are time stamped with start and finish time of the activity.



- 9.4.3.3. Such intermediate activities are defined along with outer timelines for each activity after discussion with the concerned stakeholders such as members/participants, DVP agent, participating banks, other Market Infrastructure Institutions (MIIs) etc. to achieve final pay-in and pay-out within SEBI stipulated timelines.
- 9.4.3.4. Process flow and associated timelines, so decided, are intimated to all the stakeholders and delay in completion of any of these activities, should be traceable and attributable to one or more entity / MII, as the case may be.
- 9.4.3.5. Procedures to handle various exceptions i.e. scenarios that could result in settlement delay are documented along with the steps to be taken towards completing settlement processes at the earliest in case of exceptions.
- 9.4.3.6. On the basis of the aforesaid, CCs and Depositories may separately prepare a Comprehensive Standard Operating Procedure (CSOP) which is mutually agreed upon by other CCs and Depositories as far as all the timelines and exception handling are concerned. This CSOP would be submitted to SEBI after approval of the Governing Boards of CCs and Depositories.
- 9.4.3.7. Further, the said CSOP shall also cover action points emanating from 9.4.4 below and would be reviewed periodically by the MIIs to incorporate any regulatory/system changes.

#### **9.4.4. For reporting of Delay in rolling settlement cycle**

- 9.4.4.1. In case of delay in completion of any of the intermediate activities beyond their pre-agreed time, the respective CCs/Depositories would inform the impacting CCs/Depositories regarding delay in completion of the intermediate activity at their end on immediate basis.
- 9.4.4.2. CCs shall intimate delay in settlement beyond the stipulated timelines for settlement for rolling settlement to SEBI (under intimation to depositories). This intimation should be given within one hour of such SEBI stipulated timelines and should inter-alia mention - reasons for delay, entity/MII responsible for the delay and likely completion time of the settlement process.
- 9.4.4.3. CCs and Depositories shall submit a separate report to SEBI, on a monthly basis (replacing the existing joint monthly report), wherein following details are inter-alia provided:



- 9.4.4.3.1. Day wise completion time for pay-in and pay-out activities
- 9.4.4.3.2. Details about settlement delays for the month
- 9.4.4.3.3. Intermediate activity that caused the delay and reason(s) thereof
- 9.4.4.3.4. Steps taken to address the root cause of the issue
- 9.4.4.3.5. Review of instances of delay to understand areas of improvement etc.

9.4.4.4. CCs / Depositories would also submit a report to their Governing Boards on quarterly basis with regard to instances of delay attributable to them in the said quarter. If settlement delay is on account of technical reasons, findings are to be evaluated by the SCOT of the CC / Depository before referring to the Governing Board. The report would inter-alia include the details of individual instances of settlement delay along with reasons thereof and corrective / preventive actions taken.

## **9.5. Advisory on Security Patch Management Policy**

All the MIIs are advised to ensure the following:

- 9.5.1. The security patch management policy is audited by an external auditor.
- 9.5.2. Appropriate changes, if necessary, are made to the existing policy on security patch management.

## **9.6. Standard Operating Procedure for handling of Stock Exchange Outage and extension of trading hours thereof<sup>38</sup>**

- 9.6.1. Trading hours of stock exchanges are pre-defined and known to all market participants including the other Market Infrastructure Institutions (MIIs) to enable them to carry out activities related to continuous trading in securities.
- 9.6.2. If due to any technical reason or otherwise, continuous trading on stock exchanges is disrupted, it is of paramount importance that not only all market participants including other MIIs, are promptly informed about the outage but also the trading hours are extended, if required, so as to provide opportunity for smooth closure of intraday positions.
- 9.6.3. With a view to ensure that any outage at stock exchange(s) is handled in a harmonized and consistent manner, the matter was discussed with the MIIs and Standard Operating Procedure with regard to handling of such stock exchange outage in Cash Market and Equity Derivatives segment is detailed below.

---

<sup>38</sup> Circular No. SEBI/HO/MRD-TPD-1/CIR/P/2023/7 dated January 09, 2023



### Definition of Stock Exchange Outage

9.6.4. Stock Exchange Outage shall mean stoppage of continuous trading, either suo moto by exchange or by virtue of reasons beyond control of stock exchange. Further, stoppage of continuous trading shall not include trading halt on account of index based market-wide circuit breaker.

### Reporting Requirements for outage

9.6.5. The stock exchange that suffered the outage (referred to as affected stock exchange) shall intimate about the outage to various stakeholders as mentioned below:

S No.	Communication to	Reporting
i.	Market Participants / Trading Members / Other MIIs	Immediate but not later than 15 minutes from occurrence of outage. Through broadcast message and by publishing on its website
ii.	SEBI	Immediate after occurrence of outage. Through an email to dedicated email id : <a href="mailto:techglitch@sebi.gov.in">techglitch@sebi.gov.in</a>

9.6.6. Further, the affected stock exchange shall update about the ongoing outage in the time intervals of 45 minutes from the initial intimation, as mentioned above, until normalcy to operations is restored. Extension of trading hours, if applicable (as mentioned later), shall be mentioned in the intimation by the affected stock exchange.

### Trading on unaffected segment(s) / exchanges and Resumption of trading on affected stock exchange

9.6.7. In the event of disruption of trading in one or more market segments of affected stock exchange, qualifying as outage, trading in other unaffected segments of the affected exchange shall continue and all other unaffected exchanges shall continue to trade in all of their market segments.

9.6.8. Affected stock exchange would restore operations to normalcy at the earliest including from the Disaster Recovery Site and carry out various activities, in terms of Para 9.1 and 9.3 of this Chapter of Master Circular for Stock Exchanges and Clearing Corporations.

9.6.9. A pre-opening session similar to normal pre-opening session would be conducted for effective price discovery, before resumption of trading. Further, there shall be an advance intimation of at least 15 minutes to various market participants with regard to resumption of trading or start of pre-opening session, as applicable.



**Extension of trading hours in case of outage**

- 9.6.10. If the trading on the affected stock exchange resumes to normalcy at least one hour (excluding 15 minutes of pre-opening session, if applicable) before the normal scheduled market closure, trading hours on that day for all stock exchanges would remain unchanged.
- 9.6.11. If the trading on the affected stock exchange does not resume to normalcy even one hour (excluding 15 minutes of pre-opening session, if applicable) before the scheduled market closure, trading hours for all stock exchanges would automatically get extended for additional one and half hours for that day and the same would be intimated by the affected stock exchange to market participants, other MIIs and SEBI latest by one hour fifteen minutes before the normal scheduled market closure. Subsequent to the communication from the affected stock exchange, the unaffected stock exchanges would also suitably issue a notice with regard to extension of trading hours on their stock exchanges.
- 9.6.12. If the trading on the affected stock exchange does not resume to normalcy even 45 minutes (excluding 15 minutes of pre-opening session, if applicable) post normal scheduled market closure, in the case of extension of trading hours, no further trading would be allowed on the affected stock exchange for that day and other stock exchanges would continue to operate till the extended time provided at para 11 above to enable smooth closure/settlement of intraday positions. The affected exchange would have to suitably intimate the same to market participants, other MIIs and SEBI latest by 45 minutes post normal scheduled market closure.
- 9.6.13. If the occurrence of outage as mentioned in para 4 above, happens during the last trading hour of normal operation and latest before 15 minutes of normal scheduled market closure, trading hours for all stock exchanges would automatically get extended by one and half hours for that day and the same would be intimated by the affected stock exchange to market participants, other MIIs and SEBI immediately but not later than 10 minutes from the occurrence of outage. Subsequent to the communication from the affected stock exchange, the unaffected stock exchanges would also suitably issue a notice with regard to extension of trading hours on their stock exchanges.
- 9.6.14. Exchanges have to put in place a common close out policy to ensure uniform methodology of settlement of open positions, in case continuous trading didn't happen in Cash Market or Equity Derivative Segment of the exchange during last half an hour of trading for the day due to outage.
- 9.6.15. Extension of trading hours, if any, for Cash Market would result in equivalent extension of trading hours in Equity Derivative Segment and vice versa, provided trading hours at the start of the day are aligned for both Cash Market and Equity Derivative Segment. Further, Extension of trading hours in the Cash Market would also result in equivalent extension to other secondary market mechanisms conducted during trading hours such as Offer for Sale, Buy back etc.



9.6.16. For illustration, a few scenarios pertaining to extension of trading hours are tabulated herewith with the assumptions that trading hours for two exchanges A and B in Cash Market and Equity Derivative Segment, at start of the day, are from 09:15 to 15:30 (i.e. excluding pre-opening and post-closing session) and all segments of exchange B are operating unaffected.

S No	Occurrence of outage	Event	Extension of trading hours
1	In Equity Derivative Segment of exchange A	Normalcy in the said segment restored latest by 14:30	No extension of trading hours for exchange A and B
2	In Cash Market of exchange A	Start of Pre-opening latest by 14:15	No extension of trading hours for exchange A and B
3	Any time during the trading hours in Cash Market on exchange A	Failure to start Pre-opening by 14:15 on exchange A	Trading hours in Cash Market and Equity Derivative Segment of exchange A and B extended till 17:00 and announcement in this regard to be made latest by 14:15 by the affected stock exchange. Note that such announcement is to be made on the basis of assessment by stock exchange on the likely resumption of normalcy.
		Failure to start Pre-opening by 16:00 on exchange A	No trading permitted in Cash Market on exchange A for the day. Equity Derivative Segment on exchange A and Cash Market and Equity Derivative Segment on exchange B would continue to trade till 17:00. The affected stock exchange to announce latest by 16:15.
4	At 15:05 on exchange A in Cash Market		Trading hours in Cash Market and Equity Derivative Segment of exchange A and B extended



			till 17:00 and announcement to be made by affected stock exchange within 10 minutes of occurrence of outage i.e. by 15:15
5	At 15:16 on exchange A in Cash Market		No extension of trading hours for exchange A and B

### 9.7. Testing Framework for the Information Technology (IT) Systems of the Market Infrastructure Institutions (MIIs)<sup>39</sup>

9.7.1. MIIs (i.e. Stock Exchanges, Clearing Corporations and Depositories) are systemically important institutions as they, inter-alia, provide infrastructure necessary for the smooth and uninterrupted functioning of the securities market. Therefore, it is imperative to devise a comprehensive testing framework to manage the IT systems/applications of MIIs throughout their lifecycle, which can assist the MIIs in performing thorough risk assessment before deploying any IT systems in production/ live environment.

9.7.2. Based on the recommendations of the Technology Advisory Committee (TAC), MIIs are hereby directed to ensure the following requirements while establishing the testing framework of their IT systems/applications:

- 9.7.2.1. All MIIs should do extensive testing, validation and documentation whenever new systems/ applications or changes to existing systems/applications are introduced before the deployment in production/live environment
- 9.7.2.2. A comprehensive methodology for system testing, functional testing, application security testing should be established and the same shall be approved by Standing Committee on Technology (SCOT) of respective MIIs. The scope of testing shall, inter-alia, cover business logic, system function, security controls and system performance under load and stress conditions. Any dependency on the existing systems shall be properly tested.
- 9.7.2.3. Testing should be carried out in a separate environment that replicates/mirrors the production environment in order to minimize any disruption.
- 9.7.2.4. All MIIs shall have the practice of traceability matrix to ensure that the test plan covers all intended functionality of the IT system and application.

<sup>39</sup> Circular No. SEBI/HO/MRD/TPD/P/CIR/2023/65 dated May 05, 2023



- 9.7.2.5. All MIIs shall adopt the practice of using automated testing techniques to run the test cases automatically, which may increase the depth and scope of tests and ultimately help to improve the software quality.
- 9.7.2.6. All MIIs shall establish policy/procedures on the use of third party systems/applications/software codes to ensure these systems are subject to review and testing before they are integrated with the systems of the MIIs.
- 9.7.2.7. All MIIs shall ensure that core code components operate as intended and do not produce unintended consequences. Further, any new code shall not have any impact on the existing functionality. All MIIs shall also ensure that Application Programming Interface Testing is done so that the concerned application can interact with other applications without causing disruptions of any kind.
- 9.7.2.8. All MIIs should perform regression testing for changes (e.g. enhancement, rectification, etc.) to an existing IT system to validate that it continues to function properly after the changes have been implemented. After fixing the defects found during the testing, all MIIs shall perform regression testing again to ensure that other existing functionalities are not affected during fixing the defects. All MIIs shall explore to capture the automated test cases so that regression testing can be performed multiple times with much wider coverage test cases in a short time.
- 9.7.2.9. All MIIs may institute tools to measure test/code coverage to assess comprehensiveness of the test.
- 9.7.2.10. All issues identified from testing, including system defects or software bugs, should be properly tracked and remediated immediately. Major issues that could have an adverse impact on the MII should be reported to their SCOT and addressed prior to deployment to the production environment.
- 9.7.2.11. All MIIs should ensure that the results of all testing, including results of User Acceptance Testing (UAT), that was conducted, are documented in the test report. The same shall be checked by the auditor during System and Network Audit.
- 9.7.2.12. All MIIs shall periodically conduct non-functional testing such as volume testing, resilience testing, scalability testing, performance testing, stress testing, application security testing, BCP testing, negative/destructive testing etc. for all IT systems/applications throughout their lifecycle (pre-implementation, post implementation, after changes).
- 9.7.2.13. All MIIs shall perform white box testing or structural testing, which shall inter-alia include analyzing data flow, control flow, information flow, coding practices, exception and error handling within the system.
- 9.7.3. The stock exchanges, clearing corporations and depositories are required to take necessary steps to put in place systems for implementation of the circular, including necessary amendments to the relevant bye-laws, rules and regulations, if any. The



MIIs are advised to submit the testing framework of all their IT systems after approval of SCOT.

## 9.8. Business Continuity for Clearing Corporations through Software as a Service (SaaS) Model<sup>40</sup>

9.8.1. Para 9.1 of this Chapter of Master Circular for Stock Exchanges and Clearing Corporations provides guidelines for Business Continuity Planning (BCP) and Disaster Recovery Site (DRS) for Market Infrastructure Institutions (MIIs). While DRS is meant to ensure Business Continuity of the MIIs in case of any disaster, it may have limited utility for any major malfunction of software, as software deployed at Primary Site as well as at DRS remains identical.

9.8.2. In order to strengthen the Business Continuity framework of MIIs particularly from the perspective of handling major software malfunction, discussions were held with MIIs and it was decided that in the first phase, systems would be designed to provide additional tool for business continuity in case of issues with Risk Management Systems (RMS) of CCs. The existing interoperability arrangement between CCs, mentioned at Para 4 of Chapter 6 of Master Circular for Stock Exchanges and Clearing Corporations and which resulted in increased standardization between CCs, may be leveraged to achieve this objective.

9.8.3. RMS is classified as a critical system of CC and plays an important role in ensuring smooth and uninterrupted functioning of the securities market by carrying out online real time risk management of trades happening on stock exchanges. Non-availability of RMS poses a major risk to the continuity of trading on stock exchanges. In order to further manage disruptions impacting availability of RMS, it is proposed to have another contingency measure in place under Software as a Service (SaaS) model. The framework in the first phase would operate for existing interoperable segments of CCs (Cash Market, Equity Derivatives Segment, Currency Derivatives) as follows:

### Outline of SaaS model for RMS:

9.8.4. Each CC shall design a system to run its RMS related operations, to risk manage trades for its clearing members, using the RMS related software components of another CC. This instance would be called SaaS-RMS. For instance, when NCL designs SaaS-RMS using software of ICCL, NCL would be considered as client CC and ICCL would be considered as service provider CC.

---

<sup>40</sup> SEBI/HO/MRD/TPD/P/CIR/2023/192 dated December 20, 2023



9.8.5. The arrangement between Client CC and Service Provider CC, in the context of design of SaaS-RMS shall be as below:

- 9.8.5.1. The SaaS-RMS instance would be designed to accept the trade data from exchanges; online collateral, positions etc. from the CC(s) and depository data as required from depositories. The client CC would carry out all the functions related to online real time risk management at the SaaS-RMS. This would ensure that if the SaaS-RMS is invoked by client CC, it would be in a ready state to take over operations.
- 9.8.5.2. Responsibility of service provider CC would be to provide the functioning software for RMS and that for other associated processes to the client CC. Beyond that, it would be responsibility of the client CC to operate SaaS-RMS in normal course and on the day it is invoked. Further, client CC would put in place systems to detect latency/performance issue of SaaS-RMS to flag off such anomalies to the concerned MII(s).
- 9.8.5.3. Each CC shall also make necessary arrangements for members to login to SaaS-RMS through a portal and view/add collateral and its utilization etc. in case SaaS-RMS is invoked by CC.
- 9.8.5.4. As the key purpose of the exercise is to ensure ability to risk manage trades, all the functions pertaining to risk management/collateral shall be made available by the client CC in the SaaS-RMS i.e.:

- 9.8.5.4.1. Intraday risk management of trades
- 9.8.5.4.2. Real time computation of margins and member utilization
- 9.8.5.4.3. Violation intimation to Exchanges
- 9.8.5.4.4. Response to Exchanges for orders of members in RRM
- 9.8.5.4.5. Online Custodial Participant Modifications / CP confirmations
- 9.8.5.4.6. Collateral addition by members
- 9.8.5.4.7. Receipt of Margin pledge / re-pledge data
- 9.8.5.4.8. Sending Margin pledge / re-pledge data
- 9.8.5.4.9. Member interface for Margin display, Custodial confirmations and Collateral addition/ allocation un-allocation
- 9.8.5.4.10. Handling of Early Pay-In (EPI) instructions

9.8.6. The following schematic diagram illustrates the functioning of SaaS-RMS involving exchanges, CCs and CMs:

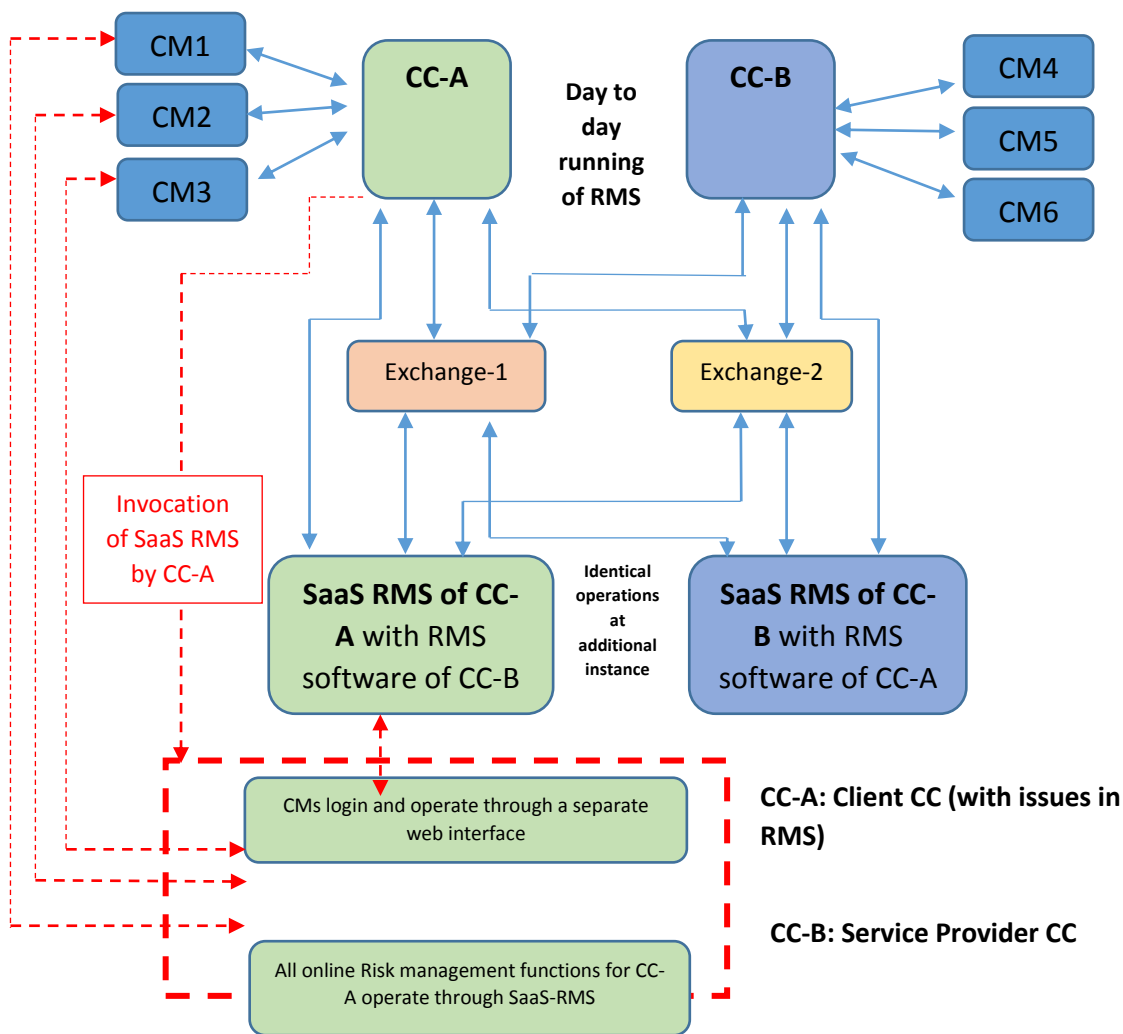


Fig1: Schematic outline of SaaS Model

9.8.7. For the purpose of illustration, the aforesaid schematic diagram considers two CCs and two exchanges wherein:

- 9.8.7.1. In normal conditions, all the RMS related activities are replicated online by both CCs in the SaaS-RMS. CMs connect to CCs through normal web interface for collateral, positions related query, updates etc.
- 9.8.7.2. Due to certain issues / malfunctioning, once CC-A decides to invoke SaaS-RMS viz. designed using RMS software of CC-B, the RMS functioning to resume by CC-A through SaaS-RMS within the timelines stipulated in the instant circular.
- 9.8.7.3. CMs of CC-A to login and operate through a separate interface provided by CC-A.



9.8.8. The aforesaid mechanism has been discussed with Technical Advisory Committee of SEBI and CCs have implemented a working model of SaaS-RMS. On the basis of test runs carried out by CCs, following timelines are stipulated:

- 9.8.8.1. A CC to take decision to shift operations to SaaS-RMS within 30 minutes of occurrence of its inability to do online real time risk management of trades at its site of functioning.
- 9.8.8.2. Within 30 minutes of the above, all allied activities such as sending violation messages to exchanges, intimating details of portal to interact with SaaS-RMS to the Clearing Members etc. to be activated through SaaS-RMS.
- 9.8.8.3. Mock session of SaaS-RMS to be carried out at least once in a quarter to familiarize and train members.

9.8.9. SaaS-RMS would be considered as a redundancy model for the CCs as part of the business continuity framework. CCs and Exchanges are therefore directed to implement the following within 30 days of the Circular:

- 9.8.9.1. To enter into an agreement laying down the roles and responsibilities of each of the entities (i.e. exchange, CCs, depositories etc.) with regard to functioning of SaaS-RMS as envisaged
- 9.8.9.2. To prepare Standard Operating Procedures covering various operational issues and edge cases related to functioning of SaaS-RMS
- 9.8.9.3. To enhance existing Interoperability Agreement to clearly demarcate roles and responsibilities of exchanges and CCs in detecting and addressing scenarios causing delay in sending/receiving the transactions data from exchanges to CCs in real time

9.8.10. The Stock Exchange, CCs and Depositories are also directed to:

- 9.8.10.1. Take necessary steps to put in place requisite infrastructure and systems for implementation of the circular, including necessary amendments to the relevant bye-laws, rules and regulations;
- 9.8.10.2. Bring the provisions of this circular to the notice of their members and also disseminate the same on its website; and
- 9.8.10.3. Communicate to SEBI, the status of implementation of the provisions of this circular.

9.8.11. Considering the above, Stock exchange and CCs are advised to submit their revised Business Continuity Policy to SEBI within two months from the date of the instant circular.



## 10. CYBER SECURITY AND CYBER RESILIENCE

### 10.1. Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporations and Depositories<sup>41</sup>

Please refer to SEBI Circular Number SEBI/HO/ITD-1/ITD\_CSC\_EXT/P/CIR/2024/113 dated August 20, 2024 on Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs).

### 10.2. Cyber Security and Cyber Resilience framework - Limited Purpose Clearing Corporation (LPCC)<sup>42</sup>

- 10.2.1. A Limited Purpose Clearing Corporation (“LPCC”) has been permitted to have arrangements with any of the existing Clearing Corporations for the purposes of Cyber Security.
- 10.2.2. The framework governing arrangements with existing Clearing Corporations for the purpose of Cyber Security is placed at Para 2 in **Annexure X**.

### 10.3. Strengthening Resiliency of Websites of Stock Exchanges, Clearing Corporations and Depositories (MIIs)

- 10.3.1. MII shall take necessary steps to ensure that its website(s) are resilient to cyber-attack(s).
- 10.3.2. Redundant websites: MII shall host its website(s) at multiple DNS (Domain Naming Servers) and hosts. MII shall put-in place suitable systems to switch to alternate website(s) hosted on a different DNS / hosts in the event of a cyber-attack on its primary website(s) and at the same time, shall take necessary steps to recover from the cyber-attack on the its primary website(s).
- 10.3.3. Web Application Firewall (WAF): MII shall mandatorily deploy Web Application firewalls of demonstrated capabilities.
- 10.3.4. Continuous monitoring of the website(s): MII shall deploy suitable and adequate resources for 24x7 monitoring of its website(s), including monitoring of their website(s) through the SOCs (Security Operations Center).

---

<sup>41</sup> Reference: Circular CIR/MRD/DP/13/2015 dated July 06, 2015, Circular SEBI/HO/MRD1/MRD1\_DTCS/P/CIR/2022/68 dated May 20, 2022 and Circular SEBI/HO/MRD/TPD/P/CIR/2023/147 dated August 24, 2023

<sup>42</sup> Circular No. SEBI/HO/MRD2/DCAP/CIR/P/227 dated November 06, 2020



- 10.3.5. MII shall periodically conduct penetration testing of its website(s) and related systems, at the minimum, once in a calendar year.
- 10.3.6. In cases where services of 3rd party vendors / service providers are availed by the MII for hosting of its website(s) and for other related areas, MII shall ensure that the cyber security and resilience framework of such 3<sup>rd</sup> party vendors / service providers are as per the requirements specified by SEBI for MIIs. Further, MII shall include audit of the cyber security and resilience framework of such 3<sup>rd</sup> party vendors / service providers (limited to the services availed by MIIs) in the scope of its annual system audit.
- 10.3.7. MII shall implement the principles mentioned in the '*Guidelines for Indian Government Websites*' developed by *National Informatics Centre (NIC)* and adopted by *Department of Administrative reforms and Public Grievances (DARPG)* on the areas of 'Website Hosting', 'Website Management', 'Development', etc. The said guidelines are available at [http://web.guidelines.gov.in/assets/documents/pdf/hand\\_book.pdf](http://web.guidelines.gov.in/assets/documents/pdf/hand_book.pdf)
- 10.3.8. MII shall frame and implement a Web Server Security Policy that should cover Network and Host Security Policy, Web Server Backup and Logging Policy, Web Server Administration and Updation Policy, Classification of documents to be published on Web Server, Password Management Policy, Encryption Policy, and Physical Security
- 10.3.9. In addition to the above, MIIs shall ensure implementation of the following:
- 10.3.9.1. MIIs shall advise their auditors to give additional emphasis on the Application Security audit.
- 10.3.9.2. MIIs shall include suitable IT / Cyber security related certifications requirements in the criteria for selection of software developers / vendors.
- 10.3.9.3. MIIs shall ensure that their software vendors undertake security audit of their systems on a periodic basis (at least once a year).

#### **10.4. Bolstering Cyber Resiliency**

- 10.4.1. In order to bolstering cyber resiliency MIIs should take following steps:
- 10.4.1.1. In addition to the current detection and prevention tools deployed at the MIIs for Network Traffic Analysis and other SIEM solutions, MIIs should start using User and Entity Behaviour Analytics (UEBA) tools for combating cyber threats.
- 10.4.1.2. The Indian-CERT has set-up a Cyber Swachhta Kendra for analyzing BOTs/malware characteristics and providing information and enabling citizens for removal of BOTs/malware. MIIs should share their public facing IPs with the Cyber Swachhta Kendra for monitoring purposes.



- 10.4.1.3. The Standing Committee on Technology (SCOT) of Exchanges and Clearing Corporations and the IT Strategy Committees (IT-CS) of Depositories should on a quarterly basis review the cyber security preparedness of the respective MIIs and also appraise the Board of MII regarding the same.
- 10.4.1.4. MIIs should place the details of Cyber-threat vectors and Cyber-attack scenarios and the corresponding action plan / steps taken to manage such threat vectors and scenarios, before its SCOT or IT-CS for assessing the adequacy of steps taken / efficacy of plans and further improvements. Thereafter, the MII should place a report in this regard before its Board before submitting the same to SEBI.
- 10.4.1.5. In addition to the periodic vulnerability assessment and penetration testing conducted by MIIs to evaluate security posture of the MII, the MIIs should also conduct periodic table-top exercises, mock drills, etc. to improve its preparedness to handle cyber breach/incident. Such exercises should be followed up with a detailed review before its SCOT or IT-CS.

#### **10.5. Comprehensive Review of Cyber Security at Stock Exchanges, Clearing Corporations and Depositories (MIIs)**

Please refer to SEBI Circular Number SEBI/HO/ITD-1/ITD\_CSC\_EXT/P/CIR/2024/113 dated August 20, 2024 on Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs).

#### **10.6. Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporations and Depositories<sup>43</sup>**

- 10.6.1. Recognizing the need for a robust Cyber Security and Cyber Resilience framework at Market Infrastructure Institutions (MIIs), i.e., Stock Exchanges, Clearing Corporations and Depositories, a detailed regulatory framework on cyber security and cyber resilience has been prescribed.
- 10.6.2. With the view to further strengthening the aforesaid framework particularly in respect of monitoring of cyber threats and cyber resiliency, the matter was discussed with SEBI's Technical Advisory Committee (TAC), SEBI's High Powered Committee on Cyber Security (HPSC-CS) and the MIIs.
- 10.6.3. Accordingly, it has been decided that MIIs shall have a Cyber Security Operation Center (C-SOC) that would be a 24x7x365 set-up manned by dedicated security analysts to identify, respond, recover and protect from cyber security incidents.

---

<sup>43</sup> Refer SEBI Circular CIR/MRD/CSC/148/2018 dated December 07, 2018



10.6.4. The C-SOC shall function in accordance with the framework specified at Para 10.1 of this Chapter of Master Circular for Stock Exchanges and Clearing Corporations. Illustrative list of broad functions and objectives to be carried out by a C-SOC are mentioned hereunder:

10.6.4.1. Prevention of cyber security incidents through proactive actions:

10.6.4.1.1. Continuous threat analysis,

10.6.4.1.2. Network and host scanning for vulnerabilities and breaches,

10.6.4.1.3. Countermeasure deployment coordination,

10.6.4.1.4. Deploy adequate and appropriate technology at the perimeter to prevent attacks originating from external environment and internal controls to manage insider threats. MIIs may implement necessary controls to achieve zero trust security model.

10.6.4.2. Monitoring, detection, and analysis of potential intrusions / security incidents in real time and through historical trending on security-relevant data sources.

10.6.4.3. Response to confirmed incidents, by coordinating resources and directing use of timely and appropriate countermeasures.

10.6.4.4. Analysis of the intrusions / security incidents (including Forensic Analysis and Root Cause Analysis) and preservation of evidence.

10.6.4.5. Providing situational awareness and reporting on cyber security status, incidents, and trends in adversary behavior to appropriate organizations including to CERT- In and NCIIPC.

10.6.4.6. Engineer and operate network defense technologies such as Intrusion Detection Systems (IDSes) and data collection / analysis systems.

10.6.4.7. MIIs to adopt security automation and orchestration technologies in C-SOC to automate the incident identification, analysis and response as per the defined procedures.

10.6.5. Further to the above, the C-SOC of MII shall, at the minimum, undertake the following activities:

10.6.5.1. In order to detect intrusions / security incidents in real time, the C-SOC should monitor and analyze on a 24x7x365 basis relevant logs of MII's network devices, logs of MII's systems, data traffic, suitable cyber intelligence (intel) feeds sourced from reliable vendors, inputs received from other MIIs, inputs received from external agencies such as CERT-In, etc. The cyber intelligence (intel) feeds may include cyber news feeds, signature updates, incident reports, threat briefs, and vulnerability alerts.



- 10.6.5.2. To this end, appropriate alert mechanisms should be implemented including a comprehensive dashboard, tracking of key security metrics and provide for cyber threat scorecards.
  - 10.6.5.3. The C-SOC should conduct continuous assessment of the threat landscape faced by the MII including undertaking periodic VAPT (Vulnerability Assessment and Penetration Testing).
  - 10.6.5.4. The C-SOC should have the ability to perform Root Cause Analysis, Incident Investigation, Forensic Analysis, Malware Reverse Engineering, etc. to determine the nature of the attack and corrective and/or preventive actions to be taken thereof.
  - 10.6.5.5. The C-SOC should conduct periodic (at the minimum quarterly) cyber attack simulation to aid in developing cyber resiliency measures. The C-SOC should develop and document mechanisms and standard operating procedures to recover from the cyber-attacks within the stipulated RTO of the MII. The C-SOC should also document various scenarios and standard operating procedures for resuming operations from Disaster Recovery (DR) site of MII.
  - 10.6.5.6. The C-SOC should conduct periodic awareness and training programs at the MII and for its members / participants / intermediaries with regard to cyber security, situational awareness and social engineering.
  - 10.6.5.7. The C-SOC should be capable to prevent attacks similar to those already faced. The C-SOC should also deploy multiple honey pot services which are dynamic in characteristics to avoid being detected as honey pot by attackers.
- 10.6.6. As building an effective C-SOC requires appropriate mix of right people, suitable security products (Technology), and well-defined processes and procedures (Processes), an indicative list of areas that MIIs should consider while designing and implementing a C-SOC are as follows:
- 10.6.6.1. The MII shall ensure that the governance and reporting structure of the C-SOC is commensurate with the risk and threat landscape of the MII. The C-SOC shall be headed by the Chief Information Security Officer (CISO) of the MII. The CISO shall be designated as a Key Managerial Personnel (KMP) and relevant provisions relating to KMPs in the *Securities Contracts (Regulation) (Stock Exchanges and Clearing Corporations) Regulations, 2018* and the subsequent circulars issued by SEBI relating to KMPs, shall apply to the CISO.
  - 10.6.6.2. While the CISO is expected to work closely with various departments of MIIs, including MII's Network team, Cyber Security team and Information Technology (IT) team, etc., the reporting of CISO shall be directly to the MD & CEO of the MII.



- 10.6.6.3. The roles and responsibilities of CISO may be drawn from Ministry of Electronics and IT notification No. 6(12)/2017-PDP-CERT-In dated March 14, 2017.<sup>44</sup>
- 10.6.6.4. The C-SOC should deploy appropriate technology tools of adequate capacity to cater to its requirements. Such tools shall, at the minimum, include Security Analytics Engine, Malware detection tools, Network and User Traffic Monitoring and Behavior Analysis systems, Predictive Threat Modelling tools, Tools for monitoring of System parameters for critical systems / servers, Deep Packet Inspection tools, Forensic Analysis tools, etc.
- 10.6.6.5. Each MII is advised to formulate a Cyber Crisis Management Plan (CCMP) based on its architecture deployed, threats faced and nature of operations. The CCMP should define the various cyber events, incidents and crisis faced by the MII, the extant cyber threat landscape, the cyber resilience envisaged, incident prevention, cyber crisis recognition, mitigation and management plan. The CCMP should be approved by the respective Standing Committee on Technology / IT- Strategy Committee of the MIIs and the governing board of the MII. The CCMP should also be reviewed and updated annually.
- 10.6.6.6. The C-SOC should have well-defined and documented processes for monitoring of its systems and networks, analysis of cyber security threats and potential intrusions / security incidents, usage of appropriate technology tools deployed by C-SOC, classification of threats and attacks, escalation hierarchy of incidents, response to threats and breaches, and reporting (internal and external) of the incidents.
- 10.6.6.7. The C-SOC should employ domain experts in the field of cyber security and resilience, network security, data security, end-point security, etc.
- 10.6.6.8. The MIIs are also advised to build a contingent C-SOC at their respective DR sites with identical capabilities w.r.t. the primary C-SOC in line with Para 9.1. Additionally, the MIIs should perform monthly live-operations from their DR-C-SOC.
- 10.6.6.9. The C-SOC should document the cases and escalation matrices for declaring a disaster.
- 10.6.7. In view of the feedback received from MIIs, it has been decided that MIIs may choose any of the following models to set-up their C-SOC:
- (i) MII's own C-SOC manned primarily by its internal staff
  - (ii) MII's own C-SOC, staffed by a service provider, but supervised by a full time staff of the MII (Refer to Clause 10.6.7.3)
  - (iii) C-SOC that may be shared by the MII with its group entities (that are also

---

<sup>44</sup> CISO roles & responsibilities - Ministry of Electronics and IT notification No. 6(12)/2017-PDP-CERT-In dated March 14, 2017



SEBI recognized MIIs)

(iv) C-SOC that may be shared by the MII with other SEBI recognized MII(s).

- 10.6.7.1. The responsibility of cyber security of an MII, adherence to business continuity and recovery objectives, etc. should lie with the respective MII, irrespective of the model adopted for C-SOC.
- 10.6.7.2. The respective risk committee(s) of the MII should evaluate the risks of outsourcing the respective activity.
- 10.6.7.3. The MII may outsource C-SOC activities in line with the guidelines as given in Annexure XIII.
- 10.6.8. A report on the functioning of the C-SOC, including details of cyber-attacks faced by the MII, major cyber events warded off by the MII, cyber security breaches, data breaches should be placed on a quarterly basis before the board of the MII.
- 10.6.9. The system auditor of the MII shall audit the implementation of the aforesaid guidance in the annual system audit of the MII. The Scope and/or Terms of Reference (ToR) of the annual system would accordingly be modified to include audit of the implementation of the aforementioned areas.
- 10.6.10. Further, in continuation to the requirement specified at Part II: Guidelines in the SEBI Circular Number SEBI/HO/ITD-1/ITD\_CSC\_EXT/P/CIR/2024/113 dated August 20, 2024 on Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs), the C-SOC shall share relevant alerts and attack information with members / participants / intermediaries of the MII, other MIIs, external cyber response agencies such as CERT-In, and SEBI.

## 10.7. Cyber Security Operations Center for SEBI registered intermediaries<sup>45</sup>

Please refer to SEBI Circular Number SEBI/HO/ITD-1/ITD\_CSC\_EXT/P/CIR/2024/113 dated August 20, 2024 on Cybersecurity and Cyber Resilience Framework for SEBI Regulated Entities (REs).

## 10.8. Reporting for Artificial Intelligence (AI) and Machine Learning (ML) applications and systems offered and used by Market Infrastructure Institutions (MIIs)<sup>46</sup>

### Background

- 10.8.1. SEBI is conducting a survey and creating an inventory of the AI / ML landscape in the Indian financial markets to gain an in-depth understanding of the adoption of such technologies in the markets and to ensure preparedness for any AI / ML policies that may arise in the future.

### Scope definition

- 10.8.2. Any set of applications/ software/ programs/ executable/ systems (computer systems) – cumulatively called application and systems, to carry out compliance operations / activities, where AI / ML is used for compliance or management purposes, is included in the scope of this circular. In order to make the scope of this circular inclusive of various AI and ML technologies in use, the scope also covers Fin-Tech and Reg-Tech initiatives undertaken by MIIs that involves AI and ML.
- 10.8.3. Technologies that are considered to be categorized as AI and ML technologies in the scope of this circular, are explained in Annexure XIV.

### Regulatory requirements

- 10.8.4. All MIIs shall fill in the AI / ML reporting form (Annexure XV) in respect of the AI or ML based applications or systems as defined in Annexure XIV offered or used by them, and submit the same in soft copy only at [AI\\_MII\\_SE@sebi.gov.in](mailto:AI_MII_SE@sebi.gov.in) (for Stock Exchanges)/ [AI\\_MII\\_DEP@sebi.gov.in](mailto:AI_MII_DEP@sebi.gov.in) (for Depositories)/ [AI\\_MII\\_CC@sebi.gov.in](mailto:AI_MII_CC@sebi.gov.in) (for Clearing Corporations) to SEBI on a quarterly basis within 15 days of the expiry of the quarter.

---

<sup>45</sup> Refer Circular CIR/MRD/CSC/151/2018 dated December 14, 2018

<sup>46</sup> SEBI Circular SEBI/HO/MRD/DoP1/CIR/P/2019/24 dated January 31, 2019

## 10.9. Standard Operating Procedure for reporting of Cyber Security breaches, incidents and deficiencies and for imposition of “Financial Disincentive” on Market Infrastructure Institutions (MIIs)

### Background

- 10.9.1. Stock exchanges, Depositories and Clearing Corporations are collectively referred to as Market Infrastructure Institutions (MIIs). These institutions are systemically important for the country’s financial development and provide the infrastructure necessary for the securities market. A smooth and uninterrupted functioning of operations of the MIIs is essential for ensuring the continuity of the securities market. It is, therefore, critical for the MIIs to constantly monitor the performance of their internal processes and systems and upgrade/ enhance their systems with respect to cyber security and cyber resilience so as to eliminate cyber security deficiencies and prevent or minimize the possibility of a cyber security breach.
- 10.9.2. However, incidents of technical and administrative lapses at MIIs have been observed some of which have arisen due to non-compliance with the extant regulatory framework for cyber security and cyber resilience and which have hindered the smooth functioning of the MIIs and threatened the continuity of the securities market. In the event of such incidents, it should be incumbent on MIIs to address cyber security deficiencies and breaches in a timely manner by taking appropriate corrective actions. It has also been observed that the MIIs were non-compliant with the extant regulatory framework for cyber security and cyber resilience in the cyber audit reports and reports from other agencies.
- 10.9.3. It has, therefore, been decided to levy a “Financial Disincentive” on MIIs in the event of the following cases:
- 10.9.3.1. Non-compliance with the extant cyber security regulations and guidelines resulting in cyber security breaches, cyber-attacks, cyber security deficiencies or any other cyber security incidents
  - 10.9.3.2. Lackadaisical approach or undue delay in addressing cyber security deficiencies and breaches
  - 10.9.3.3. Non-reporting/ delay in reporting a cyber security incident/breach

The intent of this financial disincentive is to encourage the MIIs to constantly monitor the performance of their systems and upgrade/ enhance their systems

so as to eliminate cyber security deficiencies and prevent or minimize the possibility of a cyber security breach.

- 10.9.4. In this regard, an SOP for reporting of cyber security breaches and deficiencies by MIIs and imposition of “Financial Disincentive”, is placed below for information and necessary compliance.

### **Definitions**

- 10.9.5. “*Cyber security deficiency*” shall be defined as a loophole, vulnerability or non-compliance observed in

10.9.5.1. the MII’s stated internal cyber security policy/cyber security protocol/operational guidelines/information security practices or

10.9.5.2. the cyber security guidelines specified by SEBI from time to time

which threatens or compromises the security, confidentiality, integrity or availability of the MII’s computer resource or cyber assets.

- 10.9.6. “*Cyber security incident*” shall be defined as any real or suspected adverse event in relation to cyber security that violates, explicitly or implicitly, applicable cyber security policy resulting in unauthorized access, denial of service or disruption, unauthorized use of computer resource for processing or storage of information or changes to data or information without authorization.

- 10.9.7. “*Cyber security breach*” shall be defined as any incident or security violation that results in unauthorized or illegitimate access or use by a person as well as an entity, of data, applications, services, networks and/or devices through bypass of the underlying cyber security protocols, policies and mechanisms resulting in the compromise of the confidentiality, integrity or availability of data/information maintained in a computer resource or cyber asset. A cyber security breach is a subset of a cyber security incident.

- 10.9.8. “*Information security practices*” shall be defined as implementation of cyber security policies and standards in order to minimize the cyber security incidents and cyber security breaches.

- 10.9.9. “*Cyber security policy*” shall be defined as a set of documented business rules and processes for protecting information and the computer resource.

- 10.9.10. *“Cyber security protocol”* shall be defined as the official procedure or system of rules governing the cyber security operations of a MII. The cyber security protocol is usually as subset of the cyber security policy.
- 10.9.11. *“Operational guidelines”* refers to any additional set of rules and procedures issued internally by a MII that compliments its cyber security protocol and information security practices.

### **Reporting Requirements**

- 10.9.12. The following reporting structure for cyber security deficiencies/ breach shall be adopted by the MIIs:

<b>Sl. No.</b>	<b>Issue</b>	<b>Reporting</b>
<b>1.</b>	Cyber Security Breach / Incident	<ul style="list-style-type: none"> <li>• CERT-In</li> <li>• SEBI’s Cyber Security Cell</li> <li>• Standing Committee on Technology of the MII</li> <li>• Governing Board of the MII</li> </ul>
<b>2.</b>	Cyber Security Deficiencies	<ul style="list-style-type: none"> <li>• Standing Committee on Technology of the MII</li> <li>• Governing Board of the MII</li> <li>• SEBI’s Cyber Security Cell</li> </ul>

### **Cases for levy of “Financial Disincentive”**

- 10.9.13. The “Financial Disincentive” shall be levied in the following cases:

- 10.9.13.1. Cyber security breaches, cyber-attacks and any other cyber security incidents occurring on account of non-compliance of SEBI cyber security policies and guidelines and delay in reporting the Root Cause Analysis to SEBI in case of breaches, attacks and incidents.

For the above, a “Financial Disincentive” of Rs.10,00,000/- (ten lakhs) shall be levied for

- 10.9.13.1.1. each such cyber security breach, cyber-attack or any other cyber security incident on account of non-compliance of SEBI cyber security policies and guidelines

10.9.13.1.2. delay in reporting the Root Cause Analysis to SEBI in case of such breaches, attacks and incidents.

10.9.13.1.3. for cyber security breaches, cyber-attacks and any other cyber security incidents occurring otherwise and where there is a delay in submission of the RCA report

At present SEBI has prescribed a time period of two weeks from the date of the incident for submission of RCA reports.

10.9.13.2. Cyber Security deficiencies occurring on account of non-compliance of SEBI cyber security policies and guidelines observed during biannual cyber security audits mandated by SEBI at Para 10.5 of this Chapter of Master Circular for Stock Exchanges and Clearing Corporations or reports from other agencies.

For the above, a “Financial Disincentive” of Rs.5,00,000/- (five lakhs) shall be levied for each such deficiency from the date of the report.

10.9.13.3. A cyber security breach / incident should be reported as soon as it is discovered as per the reporting structure specified in Clause 10.9.12. A “Financial Disincentive” of Rs.10,00,000/- (ten lakhs) shall be levied on those MIIs that

10.9.13.3.1. Do not report a cyber security breach/incident, or

10.9.13.3.2. Delay the reporting of the cyber security breach/incident

10.9.13.4. Failure to timely address the cyber security deficiencies / breaches within the deadline set by SEBI/ HPSC-CS. The progressive slab-wise structure for imposition of “Financial Disincentive” shall be followed from the expiry of the deadline specified by SEBI/ HPSC-CS.

<b>No. of working days post the stated deadline during which the deficiency/ cause of breach is not addressed</b>	<b>“Financial Disincentive” (Rs) per working day</b>
First 15 working days	1 lakh per working day
Subsequent 15 working days	2 lakh per working day
Subsequent working days	5 lakh per working day

10.9.14. Notwithstanding the reporting structure mentioned in Clause 10.9.12 above, the penalties would start being levied by SEBI in Clause 10.9.13 as mentioned above.

### **Proceeds to be credited to SEBI's IPEF**

10.9.15. Further, with a view to making such “Financial Disincentives” effective and meaningful, the amount realized from the same may be credited to the “Investor Protection and Education Fund” of SEBI in accordance with Section 11(1) of SEBI Act, 1992 read with Regulation 4(1)(j) of the Securities and Exchange Board of India (Investor Protection and Education Fund) Regulations, 2009, which is as follows:

Amounts to be credited to the Fund.

*“4. (1) The following amounts shall be credited to the Fund:-*

*(a)...*

*(b)...*

*(j) such other amount as the Board may specify in the interest of investors.”*

10.9.16. The “Financial Disincentive” specified above shall continue to accrue till the time the issue has been addressed by the MII by taking appropriate corrective actions and the same has been validated by an independent third party.

10.9.17. The amount of “Financial Disincentive” realized as per the above structure shall be credited by MII to Investor Protection and Education Fund administered by SEBI as mentioned in Clause 10.9.14 above.

10.9.18. Imposition of aforesaid “Financial Disincentive” shall be irrespective of any other action(s) initiated/ taken by SEBI.

### **10.10. Implementation of Cyber Capability Index**

Please refer to SEBI Circular Number SEBI/HO/ITD-1/ITD\_CSC\_EXT/P/CIR/2024/113 dated August 20, 2024 on Cybersecurity and Cyber Resilience Framework for SEBI Regulated Entities (REs).

### **10.11. Advisory on Cyber Audit and VAPT**

With regard to the cyber audit of the MIIs, the following needs to be ensured by the MIIs:

10.11.1. All MIIs should update the scope of the audit as and when any guidelines or advisory related to cyber security is issued by SEBI.

- 10.11.2. During cyber audit, evidence should be collected by inspecting physical assets, records/documents, testing of relevant systems, relevant system generated reports etc. in order to ascertain the compliance of various controls defined by SEBI.
- 10.11.3. The cyber audit report is to be submitted in the Standardized format. Please refer to SEBI Circular on CSCRF dated August 20, 2024 for the said standardised format.
- 10.11.4. Along with cyber audit reports, all MIIs are required to submit to SEBI the comments of their SCOT and Governing Board.
- 10.11.5. Scope of cyber audit shall also include testing the functional efficacy of the SOC.
- 10.11.6. VAPT exercise shall cover all possible ingress and egress points including broker ICT setup, co-location facility etc.
- 10.11.7. All MIIs shall conduct Periodic Training for the concerned employees regarding Cyber Security in line with SEBI Circular on CSCRF dated August 20, 2024 and the same has to be checked by the Auditors during cyber audit.
- 10.11.8. The audit report shall include control wise compliance of all SEBI circulars/advisories along with the evidences.
- 10.11.9. All MIIs are advised to include the directions issued by SEBI pursuant to discussion in HPSC-CS in their regular bi-annual cyber audit.
- 10.11.10. In order to ascertain the compliance of identification of critical assets as per SEBI Circular on CSCRF dated August 20, 2024, process of identification of critical assets and its implementation should be assessed during cyber audit.
- 10.11.11. For minimum baseline standards followed for conducting VAPT, please refer to SEBI Circular on CSCRF dated August 20, 2024.

All MIIs are advised to ensure the strict compliance of the said advisory and shall also bring the same to the notice of the concerned cyber auditors.

#### 10.12. **Guidelines for MIIs regarding Cyber security and Cyber resilience<sup>47</sup>**

Please refer to SEBI Circular Number SEBI/HO/ITD-1/ITD\_CSC\_EXT/P/CIR/2024/113 dated August 20, 2024 on Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs).

#### 10.13. **Advisory on encryption of Data-in motion and Data-at-rest**

As per the SEBI circular on cyber security and cyber resilience framework, MIIs are advised to ensure adoption of encryption of Data-in motion and Data-at-rest by March 31, 2024.

---

<sup>47</sup> SEBI Circular SEBI/HO/MRD/ TPD/P/CIR/2023/146 dated August 29, 2023

#### 10.14. Advisory on Cyber security and Cyber resilience

With regard to the cyber security preparedness of the MIIs, the following needs to be ensured by the MIIs:

- 10.14.1. MIIs shall ensure real-time monitoring of their IT environment with the capability of generation of real-time alerts. Logs from all servers/networks and other infrastructure shall be aggregated into SOC/SIEM and team at SOC shall proactively monitor/take actions on the alerts generated from the ingested data.
- 10.14.2. MIIs shall proactively monitor both inbound and outbound traffic.
- 10.14.3. MIIs shall build appropriate defense strategies to deal with DDoS, Insider Threat, Phishing and Ransomware-as-a-Service (“RaaS”) attacks.
- 10.14.4. MIIs should carry out employee awareness campaigns, psychometric tests, continuous face to face engagement with employees, simulation exercises etc. for employees handling critical activities/tasks to deal with any social engineering/phishing attacks.
- 10.14.5. MIIs shall physically segregate the network implemented for doing various kind of automation for physical security of building vis-à-vis networks implemented for core activities.
- 10.14.6. MIIs shall identify the vulnerabilities in their IT environment through regular scans and all critical high-impact vulnerabilities shall be closed on an urgent basis.
- 10.14.7. MIIs shall follow proper change management policy to ensure adequate testing and closure of vulnerabilities before deploying into production environment. Further, appropriate monitoring shall be done with respect to any change management implemented by MIIs.
- 10.14.8. MIIs shall ensure that they maintain online as well as offline backups of their data and appropriate testing shall be conducted on these backups to ensure confidentiality, integrity and availability.
- 10.14.9. MIIs shall ensure continuous security monitoring of third-party involvement, such as access of systems to vendors, to mitigate any cyber security risks.
- 10.14.10. MIIs shall follow the principle of zero trust architecture while providing access to IT systems. Further, MIIs shall monitor privilege access to any IT systems proactively.
- 10.14.11. MIIs should also beef up physical security of their premises.

#### 10.15. Measures taken to strengthen the cyber resilience of MIIs

Please refer to SEBI Circular Number SEBI/HO/ITD-1/ITD\_CSC\_EXT/P/CIR/2024/113 dated August 20, 2024 on Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs).

#### 10.16. Patch Management Policy of MIIs

Please refer to SEBI Circular Number SEBI/HO/ITD-1/ITD\_CSC\_EXT/P/CIR/2024/113 dated August 20, 2024 on Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs).

**Note: -Guidelines on Cybersecurity and Cyber resilience for MIIs shall be read in conjunction with SEBI Circular Number SEBI/HO/ITD-1/ITD\_CSC\_EXT/P/CIR/2024/113 dated August 20, 2024 on Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs).**

## 11. CO-LOCATION / PROXIMITY HOSTING

### 11.1. Co-location / proximity hosting facility offered by stock exchanges<sup>48</sup>

- 11.1.1. The facility of co-location or proximity hosting (or by whatever name called) is offered by the stock exchanges to stock brokers and data vendors whereby their trading or data-vending systems are allowed to be located within or at close proximity to the premises of the stock exchanges, and are allowed to connect to the trading platform of stock exchanges through direct and private network.
- 11.1.2. Based on the recommendations of SEBI's Technical Advisory Committee ("TAC"), stock exchanges are advised to follow the guidelines given below, while facilitating co-location / proximity hosting.
- 11.1.3. In order to ensure fair and equitable access to the co-location facility, stock exchanges shall:
  - 11.1.3.1. provide co-location / proximity hosting in a fair, transparent and equitable manner.
  - 11.1.3.2. ensure that all participants who avail co-location / proximity hosting facility have fair and equal access to facilities and data feeds provided by the stock exchange.
  - 11.1.3.3. ensure that all stock brokers and data vendors using co-location / proximity hosting experience similar latency with respect to exchange provided infrastructure.
  - 11.1.3.4. ensure that the size of the co-located / proximity hosting space is sufficient to accommodate all the stock brokers and data vendors who are desirous of availing the facility.
  - 11.1.3.5. provide the flexibility to avail rack space in the co-location / proximity hosting so as to meet the needs of all stock brokers desirous of availing such facility.
  - 11.1.3.6. expeditiously decide on the request of the desirous stock brokers / data vendors for availing co-location / proximity hosting and communicate the decision within fifteen working days from the receipt of the request from the stock brokers / data vendors. In case of a rejection, stock exchanges shall also provide reasons in writing to the stock brokers / data vendors.
  - 11.1.3.7. facilitate stock brokers to receive data feeds from other recognised stock exchanges at the co-location facilities and allow routing of orders to other recognised stock exchanges from the co-location facilities.

---

<sup>48</sup> Circular No. CIR/MRD/DP/07/2015 dated May 13, 2015

- 11.1.3.8. make available on their websites description of the co-location / proximity hosting, including requirements to be fulfilled by stock brokers / data vendors who avail the facility, details on fees / charges associated with the facility, etc.
  - 11.1.3.9. publish on their websites suitable quarterly reports on latencies observed at the exchange.
  - 11.1.3.10. be able to identify orders emanating from the co-located servers of stock brokers and the resultant trades. Suitable statistics relating to such orders and trades shall be disseminated by the stock exchanges.
- 11.1.4. In order to ensure that the facility of co-location / proximity hosting does not compromise integrity and security of the data and trading systems, stock exchanges shall:
- 11.1.4.1. implement suitable mechanism to protect their systems and systems of stock brokers and data vendors at co-location / proximity hosting from unauthorized access.
  - 11.1.4.2. frame guidelines on access and conduct of the personnel of stock brokers / data vendors in the premises of the stock exchange, including in the co-located space.
  - 11.1.4.3. not provide access in any form to the personnel of stock brokers/ data vendors to the stock exchange's trading platform and databases.
- 11.2. Measures to strengthen Algorithmic Trading and Co-location/ proximity Hosting Framework<sup>49</sup>**
- 11.2.1. SEBI, at Para 7 of this Chapter of Master Circular for Stock Exchanges and Clearing Corporations, has put in place the broad guidelines for algorithmic trading in the securities market. Further, SEBI, at Para 11.1 and 11.3 of this Chapter of Master Circular for Stock Exchanges and Clearing Corporations, has laid down guidelines to ensure fair and equitable access to the Co-location/proximity hosting facility offered by stock exchanges.
  - 11.2.2. In order to address the concerns relating to algorithmic trading and co- location/ proximity hosting facility offered by stock exchanges and to provide a level playing field between Algorithmic/ Co-located trading and manual trading, SEBI issued a discussion paper on August 5, 2016 requesting market participants to provide their views on the efficacy and need to introduce further mechanisms to address the aforementioned concerns.

---

<sup>49</sup> Circular No. SEBI/HO/MRD/DP/CIR/P/2018/62 dated April 09, 2018

- 11.2.3. In light of the public comments received and in consultation with Technical Advisory Committee (“TAC”) of SEBI and Secondary Market Advisory Committee (“SMAC”) of SEBI, it has been decided to introduce the following measures in connection with algorithmic trading and co-location/ proximity hosting framework facility offered by stock exchanges.

#### **Managed Co-location Service**

- 11.2.4. In order to facilitate small and medium sized Members, who otherwise find it difficult to avail colocation facility, due to various reasons including but not limited to high cost, lack of expertise in maintenance and troubleshooting, etc. to avail co-location facility, stock exchanges shall introduce ‘Managed Co-location Services’. Under this facility, space/rack in co-location facility shall be allotted to eligible vendors by the stock exchange along with provision for receiving market data for further dissemination of the same to their client members and the facility to place orders (algorithmic / non-algorithmic) by the client members from such facility.
- 11.2.5. The vendors shall provide the technical knowhow, hardware, software and other associated expertise as services to trading members and shall be responsible for upkeep and maintenance of all infrastructure in the racks provided to them.
- 11.2.6. Stock exchanges shall supervise and monitor such facilities on a continuous basis. While allowing such services, stock exchanges shall continue to abide by the provisions at Para 11.1 and 11.3 of this Chapter of Master Circular for Stock Exchanges and Clearing Corporations including remaining responsible and accountable for actions of vendors providing Managed Co-location Services and ensuring integrity, security and privacy of data, being handled at the facility.
- 11.2.7. Further, in order to have fair competition, stock exchanges are advised to ensure that multiple vendors are permitted for providing Managed Co-location Services at their co-location facility.

#### **Measurement of Latency for Co-location and Proximity Hosting**

- 11.2.8. Clause 11.1.3.9 of this Chapter of Master Circular for Stock Exchanges and Clearing Corporations mandated stock exchanges to publish suitable quarterly reports on their websites on latencies observed at the exchange.
- 11.2.9. Currently, latency is measured by the Stock Exchange as the time taken to complete the round trip from the Core Router (Core Router is the place where both Colo-location orders and Non-colocation orders meet) to the matching engine and back. In order to bring in greater transparency, stock exchanges shall additionally publish minimum, maximum and mean latencies and latencies at 50th and 99th percentile.
- 11.2.10. Stock Exchanges shall also publish reference latency, which is the time taken for an order message to travel between a reference rack in the Colocation facility and the Core Router.

**Free of Charge Tick-by-Tick Data feed (TBT Feed)**

- 11.2.11. Tick-by-Tick (TBT) data feed offered by stock exchanges provides a detailed view of the entire order-book, which includes details relating to addition, modification and cancellation of orders and trades on a real-time basis.
- 11.2.12. In order to create a more level playing field among the different types of market participants, Stock Exchanges shall provide TBT Feeds to all the trading members, free of cost, subject to trading members creating the necessary infrastructure for receiving and processing it.
- 11.2.13. After assessing the needs of the market participants, stock exchanges may increase the depth of snapshot of 5 best bid and ask quotes currently being provided by them.

**Penalty on Order to Trade Ratio (OTR)**

- 11.2.14. In order to ensure orderly trading in the market, as mentioned in Clause 7.1.2.2 of this Chapter of Master Circular for Stock Exchanges and Clearing Corporations, stock exchanges were advised to put in place effective economic disincentives for high daily order-to-trade ratio (OTR) of algo orders placed by trading members. In order to encourage algo traders to place more orders closer to the last traded price (LTP), the following modification shall be carried out in the existing OTR framework:

11.2.14.1. Instead of orders placed within  $\pm 1\%$ , orders placed within  $\pm 0.75\%$  of the LTP shall be exempted from the framework for imposing penalty for high OTR.

11.2.14.2. Orders placed in the cash segment and orders placed under the liquidity enhancement schemes shall also be brought under the OTR framework.

- 11.2.15. Further, on the basis of request received from the stock exchange(s), the following modification shall be carried out in the existing OTR framework<sup>50</sup>:

11.2.15.1. Stock exchanges may be permitted to introduce additional slabs upto OTR of 2000 (from existing OTR of 500), and for OTR more than 2000. Such slabs can be introduced with deterrent incremental penalty, which stock exchanges may decide jointly.

11.2.15.2. On the third instance of OTR being 2000 or more, in last 30 days (rolling basis), the concerned member shall not be permitted to place any orders for the first 15 minutes on the next trading day as a cooling off action.

**Unique Identifier for Algorithms / Tagging of Algorithms**

---

<sup>50</sup> Circular No. SEBI/HO/MRD1/DSAP/CIR/P/2020/107 dated June 24, 2020

- 11.2.16. Clause 7.1.7.6 of this Chapter of Master Circular for Stock Exchanges and Clearing Corporations prescribes that all algorithmic orders be tagged with a unique identifier provided by the stock exchange in order to establish audit trail.
- 11.2.17. In order to ensure enhanced surveillance, stock exchanges shall now allot a unique identifier to each algorithm approved by them. Stock exchanges shall ensure that every algorithm order reaching on exchange platform is tagged with the unique identifier allotted to the respective algorithm and that such unique identifier tags are part of the data set sent / shared with SEBI for surveillance purpose.

#### **Testing Requirement for Software and Algorithms**

- 11.2.18. Para 5.1 of this Chapter of Master Circular for Stock Exchanges and Clearing Corporations prescribes the testing procedure to be followed by market participants before deployment of software and algorithms. In order to further streamline and strengthen the process of testing of software and algorithms, stock exchanges may provide a simulated market environment for testing of software including algos. Such a facility may be made available over and beyond the current framework of mock trading prescribed by SEBI.

### **11.3. Review of guidelines for Co-location / proximity hosting facility offered by stock exchanges<sup>51</sup>**

- 11.3.1. SEBI, in consultation with Technical Advisory Committee of SEBI (TAC), has reviewed the applicable provisions regarding guidelines to be followed by stock exchanges while facilitating co-location / proximity hosting, particularly with respect to the following:
- 11.3.1.1. Direct connectivity between colocation facilities of recognized stock exchanges.
  - 11.3.1.2. Colocation services / data centre facilities entirely/ partially provided and managed by a third party data centre service provider.
  - 11.3.1.3. Stock exchanges allowing stock brokers/ data vendors to connect to the stock exchange Trading system over an internal Local Area Network (LAN).
- 11.3.2. Pursuant to the aforementioned review, stock exchanges are advised to allow direct connectivity between colocation facility of one recognised stock exchange and the colocation facility of other recognized stock exchanges. Stock exchanges are also advised to allow direct connectivity between servers of a stock broker placed in colocation facility of a recognized stock exchange and servers of the

---

<sup>51</sup> Circular No. CIR/HO/MRD/DP/CIR/P/2016/129 dated December 01, 2016

same stock broker placed in colocation facility of a different recognized stock exchange. This facility should be available to all the colocated brokers, who are desirous to avail such connectivity, in a fair and equitable manner.

- 11.3.3. In addition to the above, in order to ensure fair and equitable access to the colocation facility it is clarified as under:
- 11.3.3.1. Colocation services provided by a third party or outsourced from a third party is deemed to be provided by the stock exchanges. Stock exchange shall ensure complete control and jurisdiction over the matters related to its co-location facility. Further, stock exchange will remain responsible and accountable for actions of such outsourced entity with respect to colocation services.
  - 11.3.3.2. Stock exchanges shall submit a quarterly compliance report to SEBI regarding the outsourcing services after placing it before the board of the respective stock exchange.
  - 11.3.3.3. Facility that allows stock brokers/ data vendors to connect to the stock exchange trading system over a Local Area Network (LAN) shall fall within the definition of “Colocation / proximity hosting”.
- 11.3.4. Further, it is clarified that all provisions at Para 11.1 of this Chapter of Master Circular for Stock Exchanges and Clearing Corporations on “Colocation / proximity hosting provided by stock exchanges” shall be made applicable, including for cases such as colocation facility entirely/ partially managed by a third party and facility available to stock brokers / data vendors to connect to stock exchange’s system over LAN.

## 12. CAPACITY PLANNING

### 12.1. Capacity planning framework of stock exchanges and clearing corporations<sup>52</sup>

- 12.1.1. Being critical infrastructure of the securities market, it is imperative for the stock exchanges and clearing corporations to continuously assess and monitor their system capacities. Over the years, stock exchanges and clearing corporations have experienced increase in volumes owing to the growth of the market and have accordingly taken steps to increase capacities of their trading, clearing and settlement infrastructure.
- 12.1.2. Stock exchanges and Clearing corporations are advised to ensure the following requirements while planning capacities of their trading, clearing and settlement and risk management related infrastructure:
  - 12.1.2.1. The installed capacity shall be at least 1.5 times (1.5x) of the projected peak load.
  - 12.1.2.2. The projected peak load shall be calculated for the next 60 days based on the per-second peak load trend of the past 180 days.
  - 12.1.2.3. All systems in trading, clearing and settlement ecosystem shall be considered in this process including all technical components such as network, hardware, software, etc., and shall be adequately sized to meet the capacity requirements.
  - 12.1.2.4. In case the actual capacity utilisation exceeds 75% of the installed capacity, immediate action shall be taken to enhance the capacity.
- 12.1.3. Stock exchanges and clearing corporations shall implement suitable mechanisms, including generation of appropriate alerts, to monitor capacity utilisation on a real-time basis and shall proactively address issues pertaining to their capacity needs.

---

<sup>52</sup> Circular No. CIR/MRD/DP/17/2015 dated October 08, 2015

## 13. DATA FEEDS

### 13.1. Fair and transparent access to data feeds of the stock exchanges<sup>53</sup>

- 13.1.1. SEBI in consultation with the Technical Advisory Committee (TAC) of SEBI had reviewed the market data feed mechanism of the stock exchanges.
- 13.1.2. Based on the recommendations of SEBI's Technical Advisory Committee (TAC), it has been decided that stock exchanges shall formulate a comprehensive policy document for providing stock market related data to the market participants in a fair and transparent manner, irrespective of the type of mechanism used by the stock exchanges for broadcasting of data.
- 13.1.3. In this context, stock exchanges shall ensure that:
  - 13.1.3.1. Appropriate tools are deployed so as to monitor service quality of data feeds;
  - 13.1.3.2. Appropriate mechanism (viz. load balancers, randomizers, etc.) to manage load across systems disseminating data in order to ensure consistent response time to all market participants;
  - 13.1.3.3. All communication to the market participants, especially on all technology related matters such as Monitoring Tool, Load Balancer, Randomisation etc., are abundantly clear and precise providing all necessary details related to the concerned facility / service, including information on features, benefits, risks, etc. of the concerned facility / service, particularly for participants who have opted for colocation facility.
- 13.1.4. Further, SEBI, in Clause 7.1.2.10 of this Chapter of Master Circular for Stock Exchanges and Clearing Corporations, has directed stock exchanges to synchronize their system clocks with the atomic clock before the start of market such that their clocks have precision of at least one microsecond and accuracy of at least +/-one millisecond. In this regard, the stock exchange should ensure that all clocks of the servers and other related systems are synchronized. Stock exchanges may adopt suitable mechanism to ensure such synchronization of system clocks.

---

<sup>53</sup> Circular No. SEBI/HO/MRD/DP/CIR/P/2017/08 dated January 20, 2017

## 14. ADVISORIES RELATED TO TECHNOLOGY

### 14.1. Advisory on Technology related Investments and Planning by Market Infrastructure Institutions (MIIs)

14.1.1. The operations and functioning of MIIs are driven by technology systems, with their critical operations requiring robust technology infrastructure to enable trading, transfer/ holding of securities, clearing and settlement and information dissemination etc. as applicable. MIIs, in a sense, today can be categorized as a technology company, running a constellation of IT systems, serviced by different technology vendors.

14.1.2. Recent years have witnessed rapid pace of market development including significant growth of investor activity and market volumes. This has been coupled with evolving landscape of technology catering to securities market. Existing business processes have been increasingly getting digitized by the MIIs, due to change in market dynamics as well as Regulatory mandates. With such significant changes in the technology systems at MIIs, there is a need for upgradation of existing systems to make them up to date to cater to future growth as well as to implement Regulatory changes. It is therefore important that technology systems of MIIs keep up with the advancement and sophistication in the field of technology.

14.1.3. To ensure the aforesaid, continuous monitoring of technology infrastructure and systems, along with that of allied processes, is needed for early identification of requirements pertaining to additional investments in technology infrastructure/ systems and technology related human resources.

14.1.4. Accordingly, MIIs are advised to:

14.1.4.1. Review existing strategies/ frameworks for technology related investments/ expenses.

14.1.4.2. Formulate short term, medium term and long term Technology Investment Plan and Technology Human Resource Plan and periodically review them. Further, MIIs to ensure that such plans are pro-active, future-oriented and attuned to the criticality of technology for its functioning.

14.1.4.3. Formulate a comprehensive framework for budgeting of annual financial requirements for technology related investments/ expenses.

14.1.4.4. Review organisational structure and employee strengths across various IT/ technology related departments/verticals. This should include review of

outsourcing policies and responsibility mapping of internal staff for such outsourced functions.

- 14.1.4.5. Review internal governance frameworks, human resource strategies and risk frameworks pertaining to technology operations.

## 14.2. **Advisory on automation/review of operational processes involving IT systems of Market Infrastructure Institutions (MIIs)**

14.2.1. Rapid advancement in the field of technology, over the past few years, has not only resulted into operations of Market Infrastructure Institutions (MIIs) increasingly getting automated and executed through an array of IT systems but also into continuous upgrade/enhancements in these systems to meet technology / regulatory / business needs.

14.2.2. On the other hand, in the recent past, instances of disruption in business operations of MIIs have been observed on account of system related issues. Root cause for some of these glitches could be traced back to manual error/oversight during setting up of certain system configuration or error in executing Begin of Day (BoD) or End of Day (EoD) activities.

14.2.3. Continuous availability of systems is cornerstone of operations of the MIIs. While MIIs have business continuity policies and vendor management / outsourcing framework, adequate focus also needs to be provided to error free execution of aforesaid routine activities. Increased and effective use of automation and system driven pre-checks/alerts along with Standard Operating Procedures for routine daily activities / troubleshooting / production release of components, become critical in eliminating technology / operational risk.

14.2.4. In view of the aforesaid, MIIs are advised to:

14.2.4.1. Carry out comprehensive review of all the operational processes related to EoD and BoD activities and put in place a framework to periodically review them. The said review may be carried out from the perspective of automation of these activities, formulation of SOPs and system driven validations/monitoring alerts covering various scenarios to ensure uninterrupted and error-free functioning of systems as well as timely generation of EoD/BoD reports for members and market participants.

14.2.4.2. Put in place similar framework for one off / non-routine events/activities such as introduction of new component/functionality, troubleshooting, activities pertaining to mock trading etc.

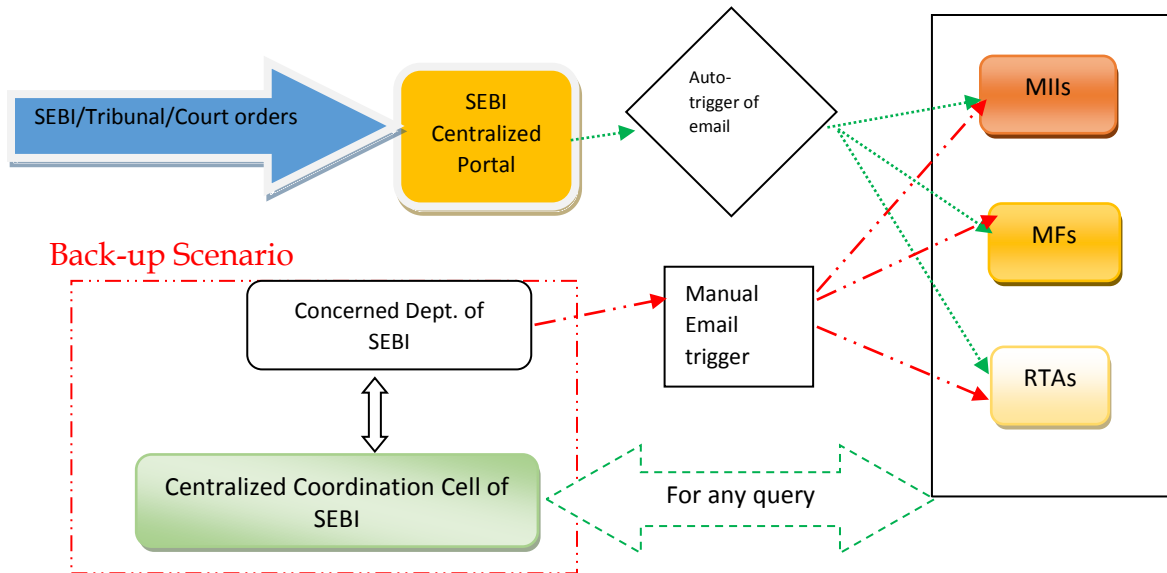
- 14.2.4.3. Ensure that all activities/processes related to or impacting system configuration, for clauses 14.2.4.1 and 14.2.4.2 above, are carried out or overseen by employee(s) of MII competent to understand the operational implications of such technical activities.
- 14.3. **Process for freezing/un-freezing of accounts/holdings pursuant to issuance of orders of SEBI/ Securities Appellate Tribunal(SAT)/ Supreme Court of India/ other courts**
- 14.3.1. At present, orders issued by SEBI and/or Hon'ble SAT/Supreme Court of India/other courts (hereinafter referred to as tribunal/court) are intimated to Market Infrastructure Institutions (MIIs), Mutual Funds(MFs) and Registrar and Transfer Agents (RTAs) for taking consequent actions by the concerned Department of SEBI.
- 14.3.2. In order to streamline and expedite the said process of taking consequent actions pursuant to issuance of orders by SEBI and/or tribunal/court, directing freezing/ un-freezing of accounts/holdings, it has been decided to introduce a new automated mechanism, which would be monitored by a Centralized Coordination Cell of SEBI. The salient features of the new mechanism are as follows: -
- 14.3.2.1. An automated process would be set up for sending intimations by SEBI to MIIs, MFs and RTAs in a standardized format from the SEBI's Case Management System(CMS) portal in respect of issuance of orders by SEBI and/or tribunal/court for freezing/un-freezing of accounts/holdings for seamless implementation of the directions.
- 14.3.2.2. A Centralized Coordination Cell under the Enforcement Department-1 (EFD-1) of SEBI has been formed to monitor/ensure timely compliance with directions for freezing/un-freezing of accounts/holdings in a time bound manner. The cell will undertake the necessary co-ordination with MIIs, MFs, RTAs and/or the concerned department of SEBI for timely implementation of the directions.
- 14.3.2.3. In order to ensure that the consequent actions pursuant to issuance of orders by SEBI and/or tribunal/court are acted upon on an immediate basis, the intimations regarding the orders of SEBI and/or tribunal/court directing freezing/ un-freezing of accounts/holdings, would be sent to the generic email IDs of MIIs, MFs and RTAs.
- 14.3.2.4. MIIs, MFs and RTAs shall establish clear ownership of their dedicated generic email ID at all times and ensure that there is due diligence at their end to

ensure compliance with orders of SEBI and/or tribunal/court in a time bound manner.

14.3.2.5. In case of any query/ further clarification required by MIIs, MFs and RTAs, they can contact the generic email ID of the Centralized Coordination Cell of EFD-1 of SEBI. The Centralized Coordination Cell would ensure that the clarification is sent to the concerned MII/MF/RTA in a time bound manner by coordinating with the concerned department of SEBI.

14.3.2.6. MIIs, MFs and RTAs shall develop the capability to generate the relevant system generated reports with respect to directions passed by SEBI and/or tribunal/court vis-a-vis actions taken by them for reconciliation/monitoring.

14.3.3. The following schematic diagram illustrates the functioning of aforesaid devised automated process:



14.3.4. In view of the above, MIIs are requested to take necessary steps to put in place requisite systems/mechanisms/framework for implementation of the above.

14.3.5. Further, MIIs are also advised to submit the compliance regarding implementation of orders of SEBI and/or tribunal/court to SEBI in the following format: -

S.No.	SEBI and/or tribunal/court order number	Date of order	Nature of directions	Implementation status (Yes or No)	Date of implementation	If not implemented, reasons for the same

**14.4. Segregation of IT Infrastructure and activities between Stock Exchanges and Clearing Corporations**

14.4.1. With respect to segregation of infrastructure between stock exchange and clearing corporation, Stock Exchanges and Clearing Corporations are advised to comply with the following:

14.4.1.1. In case of servers and storage, there should be physical segregation. Network and security can be common, but there should be logical segregation.

14.4.1.2. Infra teams should be separate and there should not be any common access to either application.

14.4.2. Further, Stock Exchanges and Clearing Corporations are hereby advised to ensure segregation of infrastructure by March 2025.

## 15. REFERENCE: List of Circulars

1. Circular no. FITTC/DC/CIR-1/98 dated June 16, 1998
2. Circular No. SMDRP/POLICY/TTA-14072/CIR-23/99 dated July 12, 1999
3. Circular No. SMD/POLICY CIR-33/99 dated October 15, 1999
4. Circular No. SMDRP/POLICY/CIR- 06/2000 dated January 31, 2000
5. Circular No. SMDRP/Policy/Cir-48/2000 dated October 11, 2000
6. Circular No. SMDRP/POLICY/CIR-56/00 dated December 15, 2000
7. Circular No. SEBI/SMD/SE/15/2003/29/04 dated April 29, 2003
8. Circular No. SEBI/MRD/Policy/SE/15864/2003 dated August 21, 2003
9. Circular No. DNPDP/ Cir-9/04 dated February 03, 2004
10. Circular No. SEBI/MRD/SE/Cir-11/2004 dated February 25, 2004
11. Ref. No. DNPDP/Cir- 22 /04 dated April 01, 2004
12. Ref. No. DNPDP/Cir-23/04 dated April 27, 2004
13. Ref. No. DNPDP/Cir-24/04 dated May 26, 2004 (STP Guidelines)
14. Ref. No. DNPDP/Cir-25/04dated June 10, 2004
15. Ref. No. DNPDP/14785/04 dated July 08, 2004
16. Ref. No. DNPDP/Cir-28/04 dated September 28, 2004
17. Circular No. MRD/DoP/SE/Cir-20/2005 dated September 8, 2005
18. Circular No. MRD/DoP/SE/Cir- 14/2006 dated September 28, 2006
19. Circular No. MRD/ DoP/SE/Cir- 7 /2008 dated April 03, 2008
20. Circular No. MRD/ DoP/SE/Cir- 03 /2009 dated February 20, 2009
21. Circular No. CIR/MRD/DP/ 25/2010 dated August 27, 2010
22. Circular No. CIR/MRD/DP/26/2010 dated August 27, 2010
23. Circular No. CIR/MRD/DP/ 36 /2010 dated December 09, 2010
24. Circular No. CIR/MRD/DP/8/2011 dated June 30, 2011
25. Circular No. CIR/MRD/DP/09/2012 dated March 30, 2012
26. Circular No. CIR/MRD/DP/20/2012 dated August 02, 2012
27. Circular No. CIR/MRD/DP/16/2013 dated May 21, 2013
28. Circular No. CIR/MRD/DP/24/2013 dated August 19, 2013
29. Circular No. CIR/MRD/DMS/34/2013 dated November 06, 2013
30. Circular No. CIR/MRD/DP/06/2014 dated February 07, 2014
31. Circular No. CIR/MRD/DP/07/2014 dated February 11, 2014
32. Circular No. CIR/MRD/DP/07/2015 dated May 13, 2015
33. Circular No. CIR/MRD/DP/13/2015 dated July 06, 2015
34. Circular No. CIR/MRD/DP/17/2015 dated October 08, 2015
35. Circular No. CIR/HO/MRD/DP/CIR/P/2016/129 dated December 01, 2016
36. Circular No. SEBI/HO/MRD/DP/CIR/P/2017/08 dated January 20, 2017

37. Circular no. SEBI/HO/MRD/DP/CIR/P/2018/62 dated April 09, 2018
38. Circular No. CIR/MRD/CSC/148/2018 dated December 07, 2018
39. Circular No. CIR/MRD/CSC/151/2018, dated December 14, 2018
40. Circular No. SEBI/HO/MRD/DoP1/CIR/P/2019/24 dated January 31, 2019
41. Circular No. SEBI/HO/MRD1/DSAP/CIR/P/2020/107 dated June 24, 2020
42. Circular No. SEBI/HO/MRD2/DCAP/CIR/P/227 November 06, 2020
43. Circular No. SEBI/HO/MRD1/DSAP/CIR/P/2020/234 November 24, 2020
44. Circular No. SEBI/HO/MRD1/DTCS/CIR/P/2021/33 March 22, 2021
45. Circular No. SEBI/HO/MRD1/DTCS/CIR/P/2021/590 dated July 05, 2021
46. Circular No. SEBI/HO/MRD1/MRD1\_DTCS/P/CIR/2022/58 dated May 02, 2022
47. Circular No. SEBI/HO/MRD1/MRD1\_DTCS/P/CIR/2022/68 dated May 20, 2022
48. Circular No. SEBI/HO/MRD-TPD-1/CIR/P/2023/7 dated January 09, 2023
49. Circular No. SEBI/HO/MRD/TPD/P/CIR/2023/65 dated May 05, 2023
50. Circular No. SEBI/HO/MRD/TPD/P/CIR/2023/147 dated August 24, 2023
51. Circular No. SEBI/HO/MRD/ TPD/P/CIR/2023/146 dated August 29, 2023
52. Circular No. SEBI/HO/MRD/TPD/P/CIR/2024/192 dated December 20, 2023
53. Circular No. SEBI/HO/MRD/TPD-1/P/CIR/2024/68 dated May 30, 2024
54. Circular No. SEBI/HO/MRD/TPD/P/CIR/2024/84 dated June 20, 2024
55. SEBI Circular SEBI/HO/MRD/TPD-1/P/CIR/2024/119 dated September 12, 2024
56. SEBI Circular SEBI/HO/MRD/TPD-1/P/CIR/2024/124 dated September 20, 2024

**Annexure I**

**TERMS AND CONDITIONS**

**PART - A: DMA FACILITY USED BY THE CLIENT**

1. The client is expected to be fully aware of the risks associated with the market and the financial instruments being traded on stock exchanges through DMA. The client shall be responsible for complying with laws, rules, regulations, notifications etc issued by regulatory authorities as may be applicable from time to time.
2. The client shall ensure that DMA facility provided by the Broker is used only to execute the trades of the client and shall not be used for transactions on behalf of any other person / entity.
3. The client shall be responsible for ensuring that, only persons authorized by it shall access and use the DMA facility provided by the Broker. All orders originating from such facility / system shall be deemed to be authorized by the client.
4. Where the client accesses or proposes to access the Broker's DMA platform through external applications, including but not restricted to services of third party service provider(s), own application(s), etc., the client shall ensure that such applications have adequate security features including but not limited to access controls, password protection etc; and that appropriate agreement(s) with such third party service provider(s) etc. for ensuring secured access and communication has been executed and are in place.
5. The client shall ensure that no person authorized by them to place orders through DMA facility provided by the broker has been / is involved in any adverse action by any regulatory authorities in any jurisdiction.
6. The client shall provide the names of authorized individual users to the broker prior to placing DMA orders.
7. The client shall not use or allow the use of DMA facility to engage in any form of market misconduct including insider trading and market manipulation or conduct that is otherwise in breach of applicable laws, rules and regulation.
8. The client is aware that Algorithmic trading i.e. generation of orders using automated execution logic is governed by Algorithmic trading guidelines issued by SEBI and Exchanges and requires prior approval of the exchanges. The client shall ensure that

new algorithms and changes to existing approved algorithms are not used through the DMA facility without prior approval of concerned stock exchanges. The client shall ensure that it has necessary checks and balances, in place to identify and control dysfunctional algorithms and the Broker shall have the right to shut down the DMA facility and remove any outstanding client orders in case of any suspected dysfunctional algo.

9. The client is aware that authentication technologies and strict security measures are required for routing orders through DMA facility and undertakes to ensure that the password of the client and/or his representative are not revealed to any third party.
10. The client acknowledges that all DMA orders placed by them through the DMA facility would be validated by the risk management system of the broker. The Broker has the right to accept or reject any DMA order placed by the client at its sole discretion.
11. The client shall be solely responsible for all acts or omissions of any person using a DMA facility and shall be bound to accept and settle all transactions executed through the DMA facility provided by the Broker notwithstanding that such order(s) may have been submitted erroneously or by an unauthorized user, or that its data is inaccurate or incomplete when submitted, or the client subsequently determines for whatever reason that the order should not have been submitted.
12. The client shall notify the Broker in the event of DMA facility being compromised. Upon receipt of this notice, client's DMA facility shall be promptly disabled but the client shall continue to be responsible for any misuse of the DMA facility or any orders placed through the DMA facility as a result of the compromise of the DMA facility at their end. The Broker shall not be liable for any loss, liability or cost whatsoever arising as a result of any unauthorized use of DMA facility at the client's end.
13. In the event of winding-up or insolvency of the client or his otherwise becoming incapable of settling their DMA obligation, broker may close out the transaction of the client as permissible under bye-laws, rules, regulations of the exchanges. The client shall continue to be liable for any losses, costs, damages arising thereof.
14. The client is fully aware of the risks of transmitting DMA orders to the Broker's DMA facility through vendor systems or service providers and the Broker is not responsible for such risks.

15. The client should be aware of the fact that neither the DMA facility will be uninterrupted nor error free nor the results that may be obtained from the use of the service or as to the timeliness, sequence, accuracy, completeness, reliability or content of any information, service or transaction provided through DMA. The DMA service is provided on an "as is", "as available" basis without warranties of any kind, either express or implied, including, but not limited to, those of information access, order execution, merchantability and fitness for a particular purpose. The Broker shall not be liable for any loss, damage or injury including but not limited to direct lost profits or trading losses or any consequential, special, incidental, indirect, or similar damages from the use or inability to use the service or any part thereof.
16. The Broker shall have the right to withdraw the DMA facility in case of:-
- Breach of the limits imposed by the broker or any regulatory authority.
  - On account of any misuse of the DMA facility by the client or on instructions from SEBI/Exchanges.
  - Any other reason, at the discretion of the broker

Broker shall endeavor to give reasonable notice to the client in such instances

17. The Broker shall not be liable or responsible for non-execution of the DMA orders of the client due to any link/system failure at the client/ Broker/ exchange(s) end.
18. This document shall not be altered, amended and /or modified by the parties in a manner that shall be in contravention of any other provisions of this document. Any additional terms and conditions should not be in contravention with rules / regulations /bye-laws/circulars, of the relevant authorities including applicable stock exchanges as amended from time to time.

## **PART - B: DMA FACILITY USED BY THE CLIENT THROUGH AN INVESTMENT MANAGER**

1. The client shall be solely responsible for all acts or omissions of any person using a DMA facility and shall be bound to accept and settle all transactions executed through the DMA facility provided by the Broker to the investment manager acting on behalf of the client, notwithstanding that such order(s) may have been submitted erroneously or by an unauthorized user, or that its data is inaccurate or incomplete when submitted, or the client subsequently determines for whatever reason that the order should not have been submitted.
2. The investment manager is expected to be fully aware of the risks associated with the market and the financial instruments being traded on stock exchanges through DMA. The investment manager shall be responsible for complying with laws, rules, regulations, notifications etc issued by regulatory authorities as may be applicable from time to time.
3. Where the DMA facility provided by the Broker is used to execute trade on behalf of one or more clients, by the investment manager, then it is represented and warranted that, at each time an order is placed by such investment manager through the DMA facility of the Broker -
  - a. The investment manager has due authority to deal on behalf of the client(s) through the Broker, specifying the roles and responsibilities of the investment manager in execution of transactions on behalf of the client(s).
  - b. The investment manager shall comply with any applicable laws, rules and regulations affecting or relating to trading operations.
  - c. The investment manager and the client(s) are bound by the terms and conditions hereof;
  - d. The investment manager using the DMA facility for routing client(s) orders shall not cross trades of their client(s) with each other. Accordingly, all orders should be offered in the market.
  - e. The stock exchange or SEBI may at any time call for any information from a client(s) or an investment manager acting on behalf of the client(s) with respect to any matter relating to the activity of the investment manager. The investment manager shall also furnish any information specifying the roles and responsibilities of the

investment manager in execution of transactions on behalf of the client(s), as and when required by the exchanges or SEBI.

4. The investment manager shall be responsible for ensuring that, only persons authorized by it shall access and use the DMA facility provided by the Broker. All orders originating from such facility / system shall be deemed to be authorized by the client.
5. Where the investment manager accesses or proposes to access the Broker's DMA platform through external applications, including but not restricted to services of third party service provider(s), own application(s), etc., the investment manager shall ensure that such applications have adequate security features including but not limited to access controls, password protection etc; and that appropriate agreement(s) with such third party service provider(s) etc. for ensuring secured access and communication has been executed and are in place.
6. The investment manager shall ensure that no person authorized by them to place orders through DMA facility provided by the broker has been / is involved in any adverse action by any regulatory authorities in any jurisdiction.
7. The investment manager shall provide the names of authorized individual users to the broker prior to placing DMA orders.
8. The investment manager shall not use or allow the use of DMA facility to engage in any form of market misconduct including insider trading and market manipulation or conduct that is otherwise in breach of applicable laws, rules and regulation.
9. The investment manager is aware that Algorithmic trading i.e. generation of orders using automated execution logic is governed by Algorithmic trading guidelines issued by SEBI and Exchanges and requires prior approval of the exchanges. The investment manager shall ensure that new algorithms and changes to existing approved algorithms are not used through the DMA facility without prior approval of concerned stock exchanges. The investment manager shall ensure that it has necessary checks and balances, in place to identify and control dysfunctional algorithms and the Broker shall have the right to shut down the DMA facility and remove any outstanding client orders in case of any suspected dysfunctional algo.
10. The investment manager is aware that authentication technologies and strict security measures are required for routing orders through DMA facility and undertakes to

ensure that the password of the investment manager and/or his representative are not revealed to any third party.

11. The investment manager acknowledges that all DMA orders placed by them through the DMA facility would be validated by the risk management system of the broker. The Broker has the right to accept or reject any DMA order placed by the investment manager at its sole discretion.
12. The investment manager shall notify the Broker in the event of DMA facility being compromised. Upon receipt of this notice, client's DMA facility shall be promptly disabled but the client shall continue to be responsible for any misuse of the DMA facility or any orders placed through the DMA facility as a result of the compromise of the DMA facility at their end. The Broker shall not be liable for any loss, liability or cost whatsoever arising as a result of any unauthorized use of DMA facility at the client's end.
13. In the event of winding-up or insolvency of the client or his otherwise becoming incapable of honoring their DMA obligation, broker may close out the transaction of the client as permissible under bye-laws, rules, regulations of the exchanges. The client shall continue to be liable for any losses, costs, damages arising thereof.
14. The investment manager is fully aware of the risks of transmitting DMA orders to the Broker's DMA facility through vendor systems or service providers and the Broker is not responsible for such risks.
15. The investment manager should be aware of the fact that neither the DMA facility will be uninterrupted nor error free nor the results that may be obtained from the use of the service or as to the timeliness, sequence, accuracy, completeness, reliability or content of any information, service or transaction provided through DMA. The DMA service is provided on an "as is", "as available" basis without warranties of any kind, either express or implied, including, but not limited to, those of information access, order execution, merchantability and fitness for a particular purpose. The Broker shall not be liable for any loss, damage or injury including but not limited to direct lost profits or trading losses or any consequential, special, incidental, indirect, or similar damages from the use or inability to use the service or any part thereof.
16. The Broker shall have the right to withdraw the DMA facility in case of:
  - a. Breach of the limits imposed by the broker or any regulatory authority.

- b. On account of any misuse of the DMA facility by the client/ investment manager or on instructions from SEBI/Exchanges.
  - c. Any other reason, at the discretion of the broker
- Broker shall endeavor to give reasonable notice to the client in such instances.

17. The Broker shall not be liable or responsible for non-execution of the DMA orders of the client due to any link/system failure at the client/Broker/exchange(s) end.

18. This document shall not be altered, amended and /or modified by the parties in a manner that shall be in contravention of any other provisions of this document. Any additional terms and conditions should not be in contravention with rules/regulations/bye-laws/circulars, of the relevant authorities including applicable stock exchanges as amended from time to time.

**Annexure II**

**On the letter head of the Investment manager**

**PART A**

DETAILS OF THE INVESTMENT MANAGER:

NAME OF THE INVESTMENT MANAGER:

NAME OF THE HOME REGULATOR:

COUNTRY OF JURISDICTION OF HOME

REGULATOR:

REGISTERED /REGULATED IN HOME

JURISDICTION AS:

SEBI REGISTRATION NUMBER:

**PART B**

CLIENT(S) DETAILS:

S. No.	Name of the entity	Name of the regulator	Regulated in India as	Registration Number	PAN

Message IFN 515 - Broker to Custodian - Contract Note - Equity

Format Sequence

**Mandatory Block A (General Information)**

Status	Field	Field Name	Content and Options	Remarks	Rules
M	16R		GENL	Start of block	
M	20C	Reference	:4!c//16x	Type of CN, Exchange number and CN No.	<p>Format: (Qualifier)/ / (References)</p> <p>Qualifier: "SEME" (4 Uppercase Characters)</p> <p>References: (Contract Type/ Exchange No. / Contract Number)</p> <p>Contract Type: A or B (1 Character Set)</p> <p>Exchange number (2 digits - e.g. Calcutta Stock Exchange will be 03)</p> <p>Contract Number: xxxxxxxxxxx (13Characters)</p> <p>The reference should not start or end with slash '/' and must not contain two consecutive slashes '//'. </p>
M	23G		4!c	To indicate new message or cancellation of a previous message	<p>Format: (Function)</p> <p>Function: "NEWM" or "CANC"</p>

O	98A	Date	:4!c//8!n	Preparation Date	Format: (Qualifier)//(Date)  Qualifier: "PREP" (4 Uppercase Characters)  Date: YYYYMMDD (8 Digits)
M	22F	Indicator	:4!c//4!c	<i>Dummy (taken since mandatory)</i>	Format: (Qualifier)//(Indicator)  Qualifier: " TRTR" (4 Uppercase Characters)  Indicator: "TRAD" (4 Uppercase Characters)

### Mandatory Subsequence A1 Linkages

M	16R		LINK	Start of block	
M	20C		:4!c//16x	To indicate the cancelled contract note (CANC). In case of NEWM, the field should contain "DUMMY"	Format: (Qualifier) // (Reference)  Qualifier: " PREV" (4 Uppercase Characters)  Reference: The reference no. as given in field SEME of the earlier contract note that is being cancelled. (16 Characters)  <i>[In case of NEWM, the field should contain "DUMMY"]</i>
M	16S		LINK	End of Block	

### End of Mandatory Subsequence A1 Linkages

M	16S		GENL	End of block	
---	-----	--	------	--------------	--

**Mandatory Block C (Confirmation details)**

M	16R		CONFDET	Start of block	
M	98A	Trade Date	:4!c//8!n	To give details of the trade date.	Format: (Qualifier)/(Date) Qualifier: "TRAD" (4 Uppercase Characters) Date: "YYYYMMDD" (8 Digits)
M	98A	Settlement Date	:4!c//8!n	To give details of the settlement date.	Format: (Qualifier) / (Date) Qualifier: "SETT" (4 Uppercase Characters) Date: "YYYYMMDD" (8 Digits)

M	90B	Price	:4!c//4!c/3!a15d	To indicate the trade rate	Format: (Qualifier)/ /(Amount Type Code)/ (Currency Code) (Price) Qualifier: "DEAL" (4 Uppercase Characters) Amount Type Code: "ACTU" (4 Uppercase Characters) Currency Code: "INR" (3 Uppercase Alphabets) Price: Upto 15 digits (including decimal places and decimal sign) comma has to be used as decimal sign and is mandatory. Integer part of amount must contain atleast one digit.
---	-----	-------	------------------	----------------------------	---

O	92A	Price	:4!c//[N]15d	To indicate brokerage rate per share	<p>Format: (Qualifier)/ /(Amount Type Code)/ (Currency Code) (Price)</p> <p>Qualifier: "CORA" (4 Uppercase Characters)</p> <p>Sign (-/+)</p> <p>Price: Upto 15 digits (including decimal places and decimal sign) comma has to be used as decimal sign and is mandatory. Integer part of amount must contain atleast one digit.</p>
M	94B	Place	:4!c//4!c/30x	To identify the exchange	<p>Format:(Qualifier)/ /(Place Code)/(Bic code / Narrative)</p> <p>Qualifier: "TRAD" (4 Uppercase Characters)</p> <p>Place Code: "EXCH" (4 Uppercase Characters)</p> <p>BIC code of the exchange will be used. Where BIC code is not available, please indicate full name of the Stock Exchange</p>

M	22H	Indicator	:4!c//4!c	To indicate whether the trade is Buy [BUYI] / Sell [SELL]	<p>Format: (Qualifier)//(Indicator)</p> <p>Qualifier: "BUSE" (4 Uppercase Characters)</p> <p>Indicator: "BUYI" or "SELL"</p>
---	-----	-----------	-----------	---	--

					(4 Uppercase Characters)
M	22H	Indicator	:4!c//4!c	To indicate where the trades is against payment [APMT] or free of payment [FREE]	Format: (Qualifier) // (Indicator) Qualifier: "PAYM" (4 Uppercase Characters) Indicator: "FREE" or "APMT" (4 Uppercase Characters)

### Mandatory Sub Block C1 (Confirmation Parties)

M	16R		CONFPTY	Start of block	
M	95Q	Party	:4!c//4*35x	To give details of the client as mentioned on the contract note.	Format: (Qualifier) //(Name, SEBI Regn No., Pan No.& Address of client.) Qualifier: "INVE" (4 Uppercase Characters) Name, SEBI Regn No., Pan No. &Address

O	97A	Account	:4!c//35x	To identify the safekeeping account. All clients need to obtain a custodian participant code.  Exchange will be identified based on 94B value in Confirmation Details irrespective of which	Format: (Qualifier) //(Custodian Participant Code) Qualifier: "SAFE" (4 Upper Characters) Custodian Participant Code: (35 Characters)
---	-----	---------	-----------	---	---

				exchange's Cust participant code is mentioned.	
--	--	--	--	--	--

M	16S		CONFPTY	End of block	
---	-----	--	---------	--------------	--

### End of Mandatory Subsequence C1 (Confirmation Parties)

M	36B	Quantity of Financial Instrument	:4!c//4!c/15d	To define the trade quantity	<p>Format: (Qualifier)/(Quantity Type Code) / (Quantity)</p> <p>Qualifier: "CONF" (4 Uppercase Characters)</p> <p>Quantity Type Code: "UNIT" (4 Uppercase Characters)</p> <p>Quantity: upto 15 digits (including decimal places and decimal sign) comma has to be used as decimal sign and is mandatory. Integer part of amount must contain atleast one digit.</p>
M	35B	Identification of Security	[ISIN1!e12!c] [4*35x]	To identify the ISIN of the Scrip and company name.	<p>Format: (Identification of Security)</p> <p>(Description of Security)</p> <p>Identification of Security: "ISIN" followed by the ISIN Code</p> <p>Description of Security: Description of the instrument(4 lines of 35 Characters)</p>

M	70E	Narrative	:4!c//10*35x	To identify Segment Type i.e. Rolling (DR) or Inter FII (DI) or Auction Rolling (AR) /Settlement Number	Format: (Qualifier) //(Narrative) Qualifier: "TPRO" (4 Upper Characters) Narrative: Line 1: "DR" or "DI" or "AR" / Settlement Number as mentioned on Stock Exchange system (35 Character Sets)
M	98C	Date/Time	:4!c//8!n6!n	To Identify order time	Format: (Qualifier) /(Date)/(Time) Qualifier: "PROC" (4 Upper Characters) Date: YYYYMMDD Time : HHMMSS
M	16S		CONFDET	End of block	

**End of Sequence C (Confirmation Details)**  
**Mandatory Sequence D (Settlement Details)**

M	16R		SETDET	Start of block	
M	22F	Indicator	:4!c//4!c	Dummy (since mandatory)	Format: (Qualifier) //(Indicator) Qualifier: "SETR" (4 Upper Characters) Indicator: "TRAD" (4 Upper Characters)

**Mandatory Subsequence D1 (Settlement Parties)**

M	16R		SETPRTY	Start of block	
---	-----	--	---------	----------------	--

M	95P	Party	:4!c//4!a2!a2!c[3!c]	Indicates the contracting broker Broker BIC code is used  <b>In case the BIC code doesn't exist</b>	Format: (Qualifier)/(BIC code of broker) Qualifier: "BUYR" in case of a Sale "SELL" in case of a Purchase BIC Code of the contracting broker
	95Q	Party	:4!c//4*35x	Indicates the Broker	Format: (Qualifier)/(Name of broker) Qualifier: "BUYR" in case of a Sale "SELL" in case of a Purchase Name: of the contracting broker
O	70C	Narrative	:4!c//4*35x	To provide additional broker contact details	Format: (Qualifier)/(Narrative) Qualifier: "PACO" (4 Uppercase Upper Characters) Narrative: Exchange Broker code! SEBI Registration Number! Address of the Broker (140 Characters)
M	70E	Narrative	:4!c//10*35x	To provide for Declaration	Format: (Qualifier)/(Narrative) Qualifier: "DECL" (4 Uppercase Upper

					<p>Characters)</p> <p>Narrative: Arbitration Clause (10 lines of 35 char each)</p> <p>Line 1: This contract is subject to Rules,</p> <p>Line 2: Byelaws and Regulations and</p> <p>Line 3: usages of (name of the exchange). In event</p> <p>Line4: of any claim (whether admitted or</p> <p>Line 5: not), difference or dispute arising</p> <p>Line 6: between you and me/us out of these</p> <p>Line 7: transactions, the matter shall be</p> <p>Line 8: referred to arbitration as provided</p> <p>Line 9: in the Rules, Byelaws and</p> <p>Line 10: Regulations of (name of the exchange).</p>
--	--	--	--	--	--

M	16S		SETPRTY	End of block	
---	-----	--	---------	--------------	--

M	16R		SETPRTY	Start of block	
---	-----	--	---------	----------------	--

M	95P	Party	:4!c//4!a2!a2!c[3!c]	Indicates who will be	Format: (Qualifier)/(BIC code of broker)
---	-----	-------	----------------------	-----------------------	--

	95Q	Party	:4!c//4*35x	<p>delivering / receiving the securities.</p> <p>In case of Clearing House Trades bic code of the Clearing Corporation will be used else in case of Hand Delivery Trade the BIC of the broker will be used.</p> <p><b>In case the BIC code doesn't exist</b></p> <p>Indicates the Delivery Type. The name of the clearing corporation is to be used in case of a clearing house trade. In case of a hand delivery trade, the brokers name is to be used.</p>	<p>Qualifier: "REAG" in case of a Sale</p> <p>"DEAG" in case of a Purchase</p> <p>BIC Code of the Clearing House (For Clearing House Trades) else</p> <p>BIC Code of the Broker (For Hand Delivery Trades)</p> <p>Format: (Qualifier)/(Name of Clearing House)</p> <p>Qualifier: "REAG" in case of a Sale</p> <p>"DEAG" in case of a Purchase</p> <p>Name of the Clearing House (For Clearing House Trades) else</p> <p>Name of the Broker (For Hand Delivery Trades)</p>
--	-----	-------	-------------	--	---

M	16S		SETPRTY	End of block	
---	-----	--	---------	--------------	--

**End of Subsequence D1 (Settlement Parties)**

**Mandatory Subsequence D3 (Amounts)**

M	16R		AMT	Start of block	
---	-----	--	-----	----------------	--

M	19A	Amount	:4!c//3!a15d	To identify the Deal Amount	<p>Format: (Qualifier) // (Currency Code) (Amount)</p> <p>For: Deal Amount</p> <p>Qualifier: "DEAL" (4 Upper case Characters)</p> <p>Narrative: "INR" (3 Upper Letters)</p> <p>Amount: upto 15 digits (including decimal places and decimal sign) comma has to be used as decimal sign and is mandatory. Integer part of amount must contain atleast one digit.</p>
---	-----	--------	--------------	-----------------------------	---

M	16S		AMT	End of block	
---	-----	--	-----	--------------	--

M	16R		AMT	Start of block	
---	-----	--	-----	----------------	--

M	19A	Amount	:4!c//3!a15d	To identify the brokerage	<p>For Brokerage:</p> <p>Qualifier: "EXEC" (4 Upper case Characters)</p> <p>Narrative: "INR" (3 Upper Letters)</p> <p>Amount: upto 15 digits (including decimal places and decimal sign) comma has to be used as decimal sign and is mandatory. Integer part of amount must contain atleast one digit.</p>
---	-----	--------	--------------	---------------------------	--

M	16S		AMT	End of block	
---	-----	--	-----	--------------	--

M	16R		AMT	Start of block	
---	-----	--	-----	----------------	--

M	19A	Amount	:4!c//3!a15d	To identify the service tax	<p>For Service Tax:</p> <p>Qualifier: "TRAX" (4 Upper case Characters)</p> <p>Narrative: "INR" (3 Upper Letters)</p> <p>Amount: upto 15 digits (including decimal places and decimal sign) comma has to be used as decimal sign and is mandatory. Integer part of amount must contain atleast one digit.</p>
---	-----	--------	--------------	-----------------------------	--

M	16S		AMT	End of block	
---	-----	--	-----	--------------	--

M	16R		AMT	Start of block	
---	-----	--	-----	----------------	--

M	19A	Amount	:4!c//3!a15d	To identify the settlement amount	<p>For Settlement Amount</p> <p>Qualifier: "SETT" (4 Upper case Characters)</p> <p>Narrative: "INR" (3 Upper Letters)</p> <p>Amount: upto 15 digits (including decimal places and decimal sign) comma has to be used as decimal sign and is mandatory. Integer part of amount must contain atleast one digit.</p>
---	-----	--------	--------------	-----------------------------------	---

M	16S		AMT	End of block	
---	-----	--	-----	--------------	--

### End of Mandatory Subsequence D3 (Amounts)

M	16S		SETDET	End of block	
---	-----	--	--------	--------------	--

### End of Sequence D Settlement Details

### Optional Sequence E (Other Parties)

M	16R		OTHRPTY	Start of block	
---	-----	--	---------	----------------	--

M	95Q	Party	:4!c//4*35x	Dummy (since mandatory)	Format: (Qualifier) //(Narrative) Qualifier: "EXCH" (4 Upper case Characters) Narrative: "ORDER DETAILS"
---	-----	-------	-------------	-------------------------	---

O	70D	Party	:4!c//6*35x	To identify the trade Ref. Number. The same field can be repeated multiple times to identify different order numbers	Format: (Qualifier) //(Narrative) Qualifier: "PART" (4 Upper case Characters) Narrative: Trade Ref. No (15 Digits) Trade Ref. Qty (15 Digits) Trade Ref. Rate (15 Digits comma at appropriate place) Date: YYYYMMDD HHMMSS (15 Character Sets)
---	-----	-------	-------------	--	--

O	20C	Reference	:4!c//16x	To identify the Order number	Format: (Qualifier) //(Reference) Qualifier: "PROC" (4 Character) Reference : Order number (16 Character Sets)
M	16S		OTHRPTY	End of block	

**----- | End of Sequence E Other Parties**

*Illustration - (IFN 515) Broker to Custodian – Contract Note – Equity*

{IFN515}{ SENDERADDRS }{ RECVERADDRS }

:16R:GENL

:20C::SEME// A0212345

:23G:NEWM

:98A::PREP// 20020828

:22F::TRTR//TRAD

:16R:LINK

:20C::PREV//DUMMY

:16S:LINK

:16S:GENL

:16R:CONFDET

:98A::SETT// 20020902

:98A::TRAD// 20020828

:90B::DEAL// ACTU/INR200,00

:94B::TRAD// EXCH/XNSEINB1XXX

:22H::BUSE//SELL

:22H::PAYM// APMT

:16R:CONFPPTY

:95Q::INVE// Client Name , Sebi Reg No

Other Details

:97A::SAFE//CLNT\_CODE  
:16S:CONFPTY  
:36B::CONF//UNIT/1000,00  
:35B:ISIN INE009A01021  
INFOSYS TECH DEM INR5.00  
:70E::TPRO//DR  
:16S:CONFDET  
:16R:SETDET  
:22F::SETR//TRAD  
:16R:SETPRTY  
:95P::BUYR//Broker BIC Code  
:70C::PACO// Exchange Broker code  
Sebi Registration Number Address of the Broker  
:16S:SETPRTY  
:16R:SETPRTY  
:95P::REAG//CCILINB1XXX  
:16S:SETPRTY  
:16R:AMT  
:19A::DEAL//INR200000,00  
:16S:AMT  
:16R:AMT  
:19A::EXEC//INR2000,00  
:16S:AMT  
:16R:AMT  
:19A::TRAX//INR100,00  
:16S:AMT  
:16R:AMT  
:19A::SETT//INR197900,00  
:16S:AMT  
:16S:SETDET

```

:16R:OTHRPTY
:95Q::EXCH//ORDER DETAILS
:70D::PART//000000000001234
000000001000,00
000000000200,00
20020822 10:20:33
:20C::PROC//123123123
:16S:OTHRPTY
-}

```

*Illustrative Example Explained - IFN 515 - Broker to Custodian – Contract Note – Equity*

Block GENL gives General information	<b>:16R:GENL</b>	
	:20C::SEME// A0212345	Indicates the contract note no Contract Type (1 Char) Exchange No. (2 Char) Contract Number
	:23G:NEWM	Indicates it is a new message
	:98A::PREP//20020828	Message preparation date
	:22F::TRTR//TRAD	
	<b>:16R:LINK</b>	
	:20C::PREV//DUMMY	For new message
	<b>:16S:LINK</b>	

		<b>:16S:GENL</b>		
Block CONFDET provides details about the trade being confirmed		<b>:16R:CONFDET</b>		
		:98A::SETT//20020902	Settlement date (Value date)	
		:98A::TRAD//20020828	Trade Date	
		:90B::DEAL//ACTU/INR200,00	Deal rate	
		:94B::TRAD//EXCH/XNSEINB1XXX	Identifies the Exchange	
		:22H::BUSE//SELL	Indicates that it's a sale transaction	
		:22H::PAYM//APMT	Indicates that the transaction is against payment	
	Confirmation Party details		<b>:16R:CONFPRTY</b>	
		:95Q::INVE// Client Name , Sebi Reg No Other Details	Provides details like client name, sebi reg no etc as provided in contract note	
		:97A::SAFE//CLNT_CODE	Indicates the client code	
			<b>:16S:CONFPRTY</b>	
			:36B::CONF//UNIT/1000,00	Indicates the Quantity of security
			:35B:ISIN INE009A01021 INFOSYS TECH DEM INR5.00	Name of the security (ISIN if available)
			:70E::TPRO//DR	Type of Trade

		<b>:16S:CONFDET</b>	
Block SETDET provides settlement details		<b>:16R:SETDET</b>	
		:22F::SETR//TRAD	
	Block SETPRTY provide details about settlement parties	<b>:16R:SETPRTY</b>	
		:95P::BUYR//Broker BIC Code :95P::REAG//CCILINB1XXX	Broker Code and that the trade is to be settled with Clearing House (CCIL)
		:70C::PACO// Exchange Broker code, Sebi Registration Number ,Address of the Broker	Broker details as provided in Contract Note
		<b>:16S:SETPRTY</b>	
	Block AMT provides details about the amounts involved	<b>:16R:AMT</b>	
		:19A::DEAL//INR200000,00	Deal amount
		:19A::EXEC//INR2000,00	Broker's commission
		:19A::TRAX//INR100,00	Service tax
:19A::SETT//INR197900,00		Settlement amount	
	<b>:16S:AMT</b>		
	<b>:16S:SETDET</b>		
Block OTHRPRTY provided details about the trade executed on the exchange	<b>:16R:OTHRPRTY</b>		
	:95Q::EXCH//ORDER DETAILS	Exchange order Number	
	:70D::PART// 000000000001234	Trade details	

	000000001000,00	
	000000000200,00	
	20020822 10:20:33	
	:20C::PROC//123123123	
	<b>:16S:OTHRPTY</b>	

**FN 515 - Broker to Custodian - Contract Note - Debt**
*Format Sequence*
*Mandatory Sequence A General Information*

<b>Status</b>	<b>Tag</b>	<b>Generic Field Name</b>	<b>Content/Options</b>	<b>Remarks</b>	<b>Rules</b>
M	16R		GENL	Start of block	
M	20C	Reference	:4!c//16x	Type of CN CN, Exchange number and CN No.	Format: (Qualifier)/ /(References)  Qualifier: "SEME" (4 Uppercase Characters)  References: (Contract Type/ Contract Number)  Contract Type: A or B (1 Character)  Exchange number (2 digits - e.g. Calcutta Stock Exchange will be 03)  Contract Number: xxxxxxxxxxx (13 Characters)

					The reference should not start or end with slash / and must not contain two consecutive slashes //.
M	23G		4!c	To indicate new/cancellation.	Format: (Function)  Function: "NEWM" or "CANC"
O	98A	Date	:4!c//8!n	Preparation Date	Format: (Qualifier)/(Date)  Qualifier: "PREP" (4 Uppercase Characters)  Date: YYYYMMDD (8 Digits)
M	22F	Indicator	:4!c//4!c	Dummy (taken since mandatory)	Format: (Qualifier)/(Indicator)  Qualifier: "TRTR" (4 Uppercase Characters)  Indicator: "TRAD" (4 Uppercase Characters)

*Mandatory Subsequence A1 Linkages*

M	16R		LINK	Start of block	
---	-----	--	------	----------------	--

M	20C		:4!c//16x	To indicate the cancelled contract note (CANC). In case of NEWM, the field should contain "DUMMY" ,	Format: (Qualifier) / (Reference)  Qualifier: " PREV" (4 Uppercase Characters)  Reference: The reference no. as given in field SEME of the earlier contract note that is being cancelled. (16 Characters)  <i>[In case of NEWM, the field should contain "DUMMY"]</i>
M	16S		LINK	End of Block	

*End of Mandatory Subsequence A1 Linkages*

M	16S		GENL	End of block	
---	-----	--	------	--------------	--

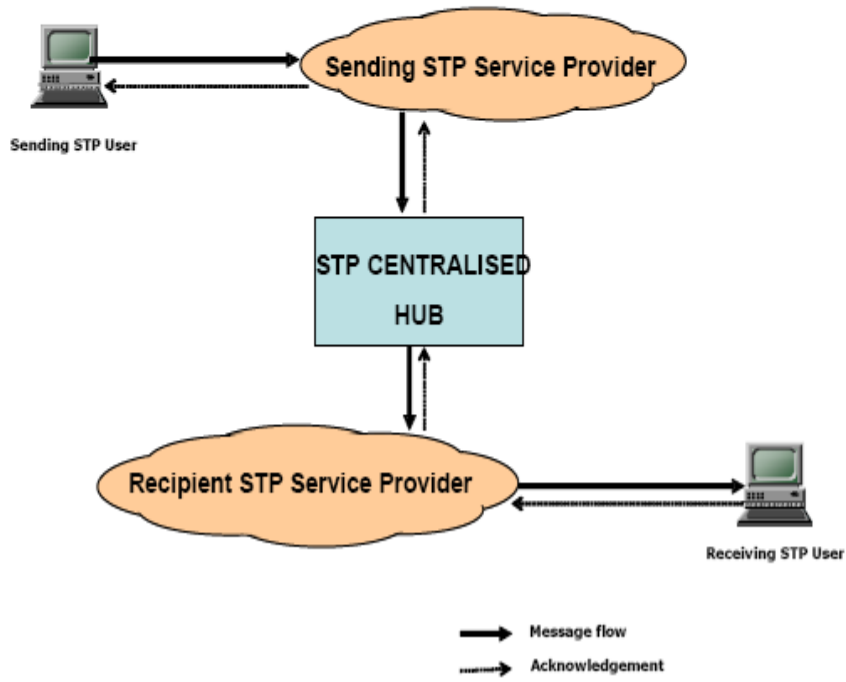
*End of Sequence A General Information*

*Mandatory Sequence C Confirmation Details*

M	16R		CONFDET	Start of block	
---	-----	--	---------	----------------	--

Annexure IV

Block Diagram of the STP System for inter STP Service Provider  
Transfer of messages



## System and Network Audit Framework

### Audit Process

1. For the System and Network Audit, the following broad areas shall be considered in order to ensure that the audit is comprehensive and effective:
  - a. The Audit shall be conducted according to the Norms, Terms of Reference (TOR) and Guidelines issued by SEBI.
  - b. The Governing Board of the Market Infrastructure Institution (MII) shall appoint the Auditors based on the prescribed Auditor Selection Norms and TOR.
  - c. An Auditor can perform a maximum of 3 successive audits. However, such auditor shall be eligible for re-appointment after a cooling-off period of two years.
  - d. Further, during the cooling-off period, the incoming auditor may not include:
    - (i) Any firm that has common partner(s) with the outgoing audit firm; and
    - (ii) Any associate/ affiliate firm(s) of the outgoing audit firm which are under the same network of audit firms wherein the term "same network" includes the firms operating or functioning, hitherto or in future, under the same brand name, trade name or common control.
  - e. The number of years an auditor has performed an audit prior to this circular shall also be considered in order to determine its eligibility in terms of sub-clause c above.
  - f. The scope of the Audit may be broadened by the Auditor to inter-alia incorporate any new developments that may arise due to issuance of circulars/ directions/ advice by SEBI from time to time.
  - g. The audit shall be conducted once in a financial year and period of audit shall be 12 months. However, for the MIIs, whose systems have been identified as "protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC), the audit shall be conducted on a half yearly basis and audit period shall be of 6 months. Further, the audit shall be completed within 2 months from the end of the audit period.

- h. In the Audit report, the Auditor shall include its comments on whether the areas covered in the Audit are in compliance with the norms/ directions/ advices issued by SEBI, internal policy of the MII, etc. Further, the audit report shall also include specific non-compliances (NCs), observations for minor deviations and suggestions for improvement. The audit report shall take previous audit reports into consideration and cover any open items therein. The auditor should indicate if a follow-on audit is required to review the status of NCs.
- i. For each of the NCs/ observations and suggestions made by the Auditor, specific corrective action as deemed fit may be taken by the MII. The management of the MII shall provide its comments on the NCs, observations and suggestions made by the Auditor, corrective actions taken or proposed to be taken along with time-line for such corrective actions.
- j. The Audit report along with the comments of management shall be placed before the Governing Board of the MII. The Audit report along with comments of the Governing Board shall be submitted to SEBI, within 1 month of completion of audit.
- k. The follow-on audit should be completed within one month of the corrective actions taken by the MII. After the follow-on audit, the MII shall submit a report to SEBI within 1 month from the date of completion of the follow-on audit. The report shall include updated Issue-Log to indicate the corrective actions taken and specific comments of the Auditor on the NCs and the corrective actions.
- l. In cases wherein follow-on audit is not required, the MII shall submit an Action Taken Report (ATR) to the Auditor. After verification of the ATR by the Auditor, the MII shall submit a report to SEBI within 1 month from the date of completion of verification by the Auditor. The report shall include updated Issue-Log to indicate the corrective actions taken and specific comments of the auditor on the ATR.
- m. The overall timeline from the last date of the audit period till completion of final compliance by MII, including follow-on audit, if any, should not exceed one year/6 months (as applicable). In exceptional cases, if MII is of the view that compliance with certain observations may extend beyond said period, then the concerned MII shall seek specific approval from the Governing Board.

## Auditor Selection Norms

2. MII shall ensure compliance with the following norms while appointing Auditor:
  - a. The auditor must have minimum 3 years of demonstrable experience in IT audit of securities market participants e.g. stock exchanges, clearing corporations, depositories, intermediaries, etc. and/ or financial services sector i.e. banking, insurance, Fin-tech etc.
  - b. The team performing system and network audit must have experience in / direct access to experienced resources in the areas covered under TOR. It is recommended that resources deployed by the Auditor for the purpose of system and network audit shall have relevant industry recognized certifications e.g. CISA (Certified Information Systems Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, GSNA (GIAC Systems and Network Auditor), CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium, commonly known as (ISC).
  - c. The Auditor shall have experience in working on Network Audit/IT audit/governance/IT service management frameworks and processes conforming to industry leading practices like CobiT/ ISO 27001 and beyond.
  - d. The Auditor should have the capability to undertake forensic audit and undertake such audit as part of system and network audit, if required.
  - e. The Auditor must not have any conflict of interest in conducting fair, objective and independent audit of the exchange / depository/ clearing corporation. It should not have been engaged over the last three years in any consulting engagement with any departments / units of the entity being audited.
  - f. The Auditor should not have any cases pending against it, which point to its incompetence and/or unsuitability to perform the audit task.
  - g. The proposed audit agency must be empanelled with CERT-In.
  - h. Any criteria, in addition to the aforesaid criteria, that the MII may deem fit for the purpose of selection of Auditor.

### **Audit Report Guidelines**

3. The Audit report should cover each of the major areas mentioned in the TOR and compliance with SEBI circulars/directions/advice, etc. related to technology. The Auditor in the Audit Report shall give its views indicating the NCs to the standards or observations or suggestions. For each section, auditors should also provide qualitative inputs/suggestions about ways to improve the processes, based upon the best industry practices.
4. The auditor shall certify that entire network architecture, connectivity (including co-located facility) and its linkage to the trading infrastructure are in conformity with SEBI's regulatory framework to provide fair equitable, transparent and non-discriminatory treatment to all the market participants.
5. The report should also include tabulated data to show NCs / observations for each of the major areas in the TOR.
6. The audit report to include point-wise compliance of areas prescribed in Terms of Reference (TOR) and areas emanating from relevant SEBI circulars/directions/advice along with any accompanying evidence.
7. Evidences should be specified in the audit report while reporting/ closing an issue.
8. A detailed report with regard to the system and network audit shall be submitted to SEBI. The report shall include an Executive Summary as per the following format:

<b>Issue Log Column Heading</b>	<b>Description</b>	<b>Responsibility</b>
<b>Major Area</b>	Comprehensive identification of major areas in compliance with various SEBI circulars / norms and internal policies of MII	Auditor/ Auditee
<b>Point wise Compliance</b>	Point-wise list of areas/relevant clauses in TOR against which compliance is being audited (in tabular format)	Auditor
<b>Description of Finding/ Observation</b>	Describe the findings in sufficient detail, referencing any accompanying evidence (e.g. procedure manual, interview notes, reports etc.)	Auditor
<b>Reference</b>	Reference to the section in detailed report - where full background information about the findings are available	Auditor
<b>Process/ Unit</b>	Process or unit where the audit is conducted and the finding pertains to	Auditor
<b>Category of Findings</b>	Major/Minor Non-compliance, Observation, Suggestion etc.	Auditor
<b>Audited By</b>	Which Auditor covered the findings	Auditor
<b>Root Cause Analysis</b>	A detailed analysis on the cause of the Non-compliance	Auditee
<b>Remediation</b>	The action (to be) taken to correct the Non-compliance	Auditee
<b>Target Completion Date for Remedial Action</b>	The date by which remedial action must be/will be completed	Auditor/ Auditee
<b>Status</b>	Status of finding on reporting date (open/close)	Auditor/ Auditee
<b>Verified By</b>	Auditing personnel (upon verification that finding can be closed)	Auditor
<b>Closing Date</b>	Date when finding is verified and can be closed	Auditor

**System and Network Audit Program – Terms of Reference (TOR)**

1. The scope of audit shall encompass all the IT resources including hardware, software, network, policies, procedures etc. of MIIs (Primary Data Centre (PDC), Disaster Recovery Site (DRS) and Near Site (NS)).
2. **IT environment**
  - 2.1. Organization details
    - a. Name
    - b. Address
    - c. IT team size (in house- employees)
    - d. IT team size (vendors)
  - 2.2. IT and network set up and usage
    - a. PDC, DRS, NS and Regional/ Branch offices (location, owned/ outsourced)
    - b. Connectivity amongst PDC, NS and DRS
    - c. IT infrastructure / applications pertaining to the activities done as a MII
    - d. System Architecture
    - e. Network Architecture
    - f. Telecommunication network
3. **IT Governance**
  - 3.1. Whether IT Governance framework exists to include the following:
    - a. IT organization structure including roles and responsibilities of key IT personnel;
    - b. IT governance processes including policy making, implementation and monitoring to ensure that the governance principles are followed;
  - 3.2. IT policies and procedures
    - a. Whether the organization has a defined and documented IT policy? If yes, is it approved by the Governing Board (GB)?
    - b. Is the current System Architecture including infrastructure, network and application components describing system linkages and dependencies, documented?
    - c. Whether defined and documented Standard Operating Procedures (SOPs) for the following processes are in place?
      - i. IT Assets Acquisition

- ii. Access Management
- iii. Change Management
- iv. Backup and Recovery
- v. Incident Management
- vi. Problem Management
- vii. Patch Management
- viii. Data Centre Operations
- ix. Operating Systems and Database Management
- x. Network Management
- xi. DRS Operations
- xii. Data Retention and Disposal
- xiii. Asset Inventory
- xiv. IT asset refresh/replacement policy
- xv. Database Security
- xvi. Interface Security
- xvii. Application Security
- xviii. Password Security
- xix. Archived and Backed up Data Security

3.3. Whether the above mentioned SOPs is reviewed at periodic intervals or upon the occurrence of any major event? In this regard, whether any organization policy has been formulated by the MII?

#### 4. Business Controls

##### 4.1. General Controls for Data Centre Facilities

- a. Application Access – segregation of duties, database and application access etc. (Approved Policy clearly defining roles and responsibilities of the personnel handling business operations)
- b. Maintenance Access – vendor engineers
- c. Physical Access Controls – permissions, logging, exception reporting & alerts
- d. Environmental Controls – fire protection, AC monitoring, etc.
- e. Fault Resolution Mechanism
- f. Folder Sharing and Back Up Controls – safeguard of critical information on local desktops
- g. Incidences of violations in the previous audit report and corrective action(s), if any, taken
- h. Any other controls, as deemed fit, by the MII

##### 4.2. Software change control

- a. Whether pre-implementation review of application controls (including controls over change management) was undertaken?
- b. Adherence to secure Software Development Life Cycle (SDLC) / Software Testing Life Cycle (STLC) standards/ methodologies
- c. Whether post implementation review of application controls was undertaken?
- d. Is the review of processes to ensure data integrity post implementation of new application or system followed by implementation team?
- e. User awareness
- f. Processing of new feature request
- g. Fault reporting / tracking mechanism & process for resolutions
- h. Testing of New releases / Bug-fixes – Testing process (automation level)
- i. Version Control – History, Change Management process etc.
- j. Development / Test/ Production environment – Segregation
- k. New Release in Production – Promotion, Release note approvals
- l. Production Issues / disruptions reported in the previous audit report, root cause analysis & corrective actions taken, if any
- m. Software Development Stage
- n. Software Design to ensure adequate system capacity to enable functioning in a degraded manner in the event of a crash
- o. Any other controls, as deemed fit, by the MII

#### 4.3. Data Communication/ Network Controls

- a. Network Administration – Redundancy, Monitoring, breakdown resolution etc.
- b. WAN Management – Connectivity provisions for business continuity
- c. Encryption - Router based as well as during transmission
- d. Connection Permissions – Restriction on need to have basis
- e. Fallback Mechanism – Dial-up connections controls etc.
- f. Hardware based Signing Process
- g. Incidences of access violations in the previous report & corrective actions taken, if any
- h. Any other controls, as deemed fit, by the MII

#### 4.4. Security Controls

- a. Secured e-mail with other entities such as SEBI, other partners
- b. Email Archival Implementation

#### 4.5. Access Policy and Controls

- a. Defined and documented policies and procedures for managing access to applications and infrastructure – PDC, DRS, NS, branches (including network, operating systems and database) and approved by relevant authority
- b. Review of access logs
- c. Access rights and roles review procedures for all systems
- d. Segregation of Duties (SOD) matrix describing key roles
- e. Risk acceptance for violation of SOPs and alternate mechanism put in place
- f. Privileged access to system and record of logs,
- g. Periodic monitoring of access rights for privileged users
- h. Authentication mechanisms used for access to systems including use of passwords, One Time Passwords (OTP), Single Sign on, etc.
- i. Any other controls, as deemed fit, by the MII

#### 4.6. Electronic Document Controls

#### 4.7. General Access Controls

#### 4.8. Performance Audit

- a. Comparison of changes in transaction volumes since previous audit
- b. Review of systems (hardware, software, network) performance over the period
- c. Review of the current volumes against the last performance test and against the current system utilization

#### 4.9. Business Continuity / Disaster Recovery Facilities

- a. a. Business Continuity Planning (BCP) manual, including Business Impact Analysis (BIA), Risk Assessment and Disaster Recovery (DR) process, Roles and responsibilities of Incident Response Team (IRT) /Crisis Management Team (CMT), employees, support/outsourced staff
- b. Implementation of policies
- c. Back-up procedures and recovery mechanism using back-ups
- d. Storage of Back-up (Remote site, DRS etc.)
- e. Redundancy – Equipment, Network, Site etc.
- f. DRS installation and Drills - Management statement on targeted resumption capability (in terms of time required & extent of loss of data)
- g. Evidence of achieving the set targets during the DR drills in event of various disaster scenarios
- h. Debrief / review of any actual event when the DR/BCP was invoked during the year
- i. User awareness and training
- j. Is Recovery Time Objective (RTO) /Recovery Point Objective (RPO) during BIA documented?

- k. Is annual review of BCP-DR or in case of major change in business/ infrastructure undertaken?
- l. Is quarterly review regarding implementation of BCP policy done by Standing Committee of Technology (SCOT) of the MII?
- m. Testing of BCP-DR plan through appropriate strategies including simulations, DR drills, system recovery, etc.
- n. Is the recordkeeping of quarterly DR drills, live trading sessions from DRS being maintained?
- o. Is BCP-DR policy document prepared and implemented in line with SEBI circular on BCP and DR of MII?

#### 4.10. IT/Network Support & IT Asset Management

- a. Utilization Monitoring – including report of prior year utilization
- b. Capacity Planning – including projection of business volumes
- c. Capacity and performance management process for the network/systems
- d. IT (S/W, H/W & N/W) Assets, Licenses & maintenance contracts
- e. Comprehensive review of Assets life cycle management (Acquisition, commissioning, deployment, monitoring, maintenance and de commissioning) and relevant records related to it.
- f. Insurance
- g. Disposal – Equipment, media, etc.

- 5. Entity Specific Software used for or in support of trading/clearing systems / peripheral systems and critical processes

#### 6. Human Resources Management

- 6.1. Screening of Employee, Third party vendors / contractors
- 6.2. Onboarding
- 6.3. Offboarding
- 6.4. Consequence Management (Incident / Breach of policies)
- 6.5. Awareness and Trainings
- 6.6. Non-Disclosure Agreements (NDAs) and confidentiality agreement

#### 7. Network Audit

- 7.1. The audit shall cover entire network infrastructure which shall inter-alia includes physical verification and tracing of the connectivity paths, server configuration,

physical checking wire to wire connectivity and configurations of computer networking devices etc.

- 7.2. The audit shall require tracing of the connectivity and network diagram based on the physical audit.
  - 7.3. The audit shall cover the link, the path, device-level redundancy, no single-point failures, high availability, and fault tolerance aspects in the network.
  - 7.4. The audit shall cover entire network that is used to connect members to the MIIs (POP, MPLS, VSAT, COLO, etc.)
  - 7.5. The audit shall cover applications, internal networks, servers, etc. of the MIIs/offered by the MIIs to its members that are used for trading, risk management, clearing and settlement etc.
  - 7.6. Network performance and design
  - 7.7. Network Security implementation
  - 7.8. Network health monitoring and alert system
  - 7.9. Log management process
  - 7.10. Service level definition for vendors/Service level management
  - 7.11. Governance process for network service delivery by vendors
8. The results of all testing that was conducted before deployment of any IT system/application in production environment, shall be checked by auditor during system audit.
9. **IT Vendor Selection and Management**
    - 9.1. Identification of eligible vendors
    - 9.2. Dissemination process of Request for Proposal (RFP)
    - 9.3. Definition of criteria of evaluation
    - 9.4. Process of competitive analysis
    - 9.5. Approach for selection
    - 9.6. Escrow arrangement for keeping source code

**10. E-Mail system**

- 10.1. Existence of policy for the acceptable use of electronic mail
- 10.2. Regulations governing file transfer and exchange of messages with external parties
- 10.3. Rules based on which e-mail addresses are assigned
- 10.4. Storage, backup and retrieval

**11. Redressal of Technological Complaints**

- 11.1. Ageing analysis of technology complaints
- 11.2. Whether all complaints received are brought to their logical conclusion?

**12. Any other Item(s)**

- 12.1. Electronic Waste Disposal
- 12.2. Observation(s) based on previous Audit Report(s)
- 12.3. Any other specific area(s) that may be informed by SEBI.

### Annexure VII

**Format for monitoring compliance with requirements emanating from SEBI circulars/guidelines/advisories related to technology**

<b>Sl. No.</b>	<b>Date of SEBI circular/ directions/ advice, etc.</b>	<b>Subject</b>	<b>Technological requirements specified by SEBI in brief</b>	<b>Mechanism put in place by the MIIs</b>	<b>Non compliances with SEBI circulars / directions, etc.</b>	<b>Compliance status (Open/ closed)</b>	<b>Comments of the Management</b>	<b>Time-line for taking corrective action in case of open observations</b>

### Annexure VIII

#### Exception Observation Reporting Format

**Note:** MIIs are expected to submit following information with regard to exceptional major non-compliances (NCs) / minor NCs observed in the System and Network Audit. MIIs should also categorically highlight those observations/NCs/suggestions pointed out in the System and Network Audit (current and previous) which are not yet complied with.

Name of the MII: \_\_\_\_\_

Name of the Auditor: \_\_\_\_\_

System and Network Audit Report Date: \_\_\_\_\_

**Table 1: For preliminary audit**

Audit period	Observation No.	Description of finding	Department of MII	Status/Nature of finding	Risk Rating of finding as per Auditor	Audit TOR clause	Root Cause Analysis	Impact Analysis	Corrective Actions proposed by auditor	Deadline for the corrective action	Management response in case of acceptance of associated risks	Whether similar issue was observed in any of the previous 3 Audits

**Description of relevant Table heads**

1. **Audit Period** – This indicates the period of audit
2. **Description of findings/observations** – Description of the findings in sufficient details, referencing any accompanying evidence
3. **Status/ Nature of Findings** – The category can be specified for example:
  - a. Non-compliant (Major/Minor)
  - b. Work in progress
  - c. Observation
  - d. Suggestion
4. **Risk Rating of finding** - A rating has to be given for each of the observations based on its impact and severity to reflect the risk exposure as well as the suggested priority for action

<b>Rating</b>	<b>Description</b>
<b>HIGH</b>	Represents weakness in control with respect to threat(s) that is /are sufficiently capable and impacts asset (s) leading to regulatory non-compliance, significant financial, operational and reputational loss. These observations need to be addressed with utmost priority.
<b>MEDIUM</b>	Represents weakness in control with respect to threat(s) that is /are sufficiently capable and impacts asset (s) leading to exposure in terms of financial, operational and reputational loss. These observations need to be addressed in reasonable timeframe.
<b>LOW</b>	Represents weaknesses in control, 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 non-conformity.
7. **Impact Analysis** – An analysis of the likely impact on the operations/ activity of the organization
8. **Corrective Action** – The action taken to correct the non-conformity

**Table 2: For follow on/ follow up system audit**

Preliminary Audit Date	Preliminary Audit Period	Preliminary Observation Number	Preliminary Status	Preliminary Corrective Action as proposed by Auditor	Current Finding	Current Status	Revised Corrective Action, if any	Deadline for the Revised Corrective Action	Reason for delay in implementation / compliance

**Description of relevant Table heads**

- 1. Preliminary Status** - The original finding as per the preliminary System and Network Audit Report
- 2. Preliminary Corrective Action** - The original corrective action as prescribed in the preliminary System and Network Audit Report
- 3. Current Finding** - The current finding w.r.t. the issue
- 4. Current Status** - Current Status of the issue viz. compliant, non-compliant, work in progress (WIP)
- 5. Revised Corrective Action** - The revised corrective action prescribed w.r.t. the Non-compliant/ WIP issues

\*\*\*\*\*

## Stock Broker System Audit Framework

### Audit Process

1. System Audit of stock brokers should be conducted with the following periodicity:
  - a. Annual system audit is prescribed for stock brokers who satisfy any of the following criteria.
    - i. Stock Brokers who use [Computer-to-Computer Link (CTCL) or Intermediate Messaging Layer (IML)]<sup>54</sup> / Internet Based Trading (IBT)/ Direct Market Access (DMA)/ Securities Trading using Wireless Technology (STWT) / Smart Order Routing (SOR) and have presence in more than 10 locations or number of terminals are more than 50.
    - ii. Stock Brokers who are depository participants or are involved in offering any other financial services.
  - b. Half yearly system audit has been prescribed for stock brokers who use Algorithmic Trading or provide their clients with the facility of Algorithmic Trading as per SEBI Circular CIR/MRD/16/2013 dated May 21, 2013.
  - c. For all other stock brokers, system audit shall be conducted once in two years.
2. Such audit shall be conducted in accordance with the Norms, Terms of Reference (ToR) and Guidelines issued by SEBI and / or by stock exchanges. Separate ToRs are specified for the following categories of brokers:
  - a. **Type I Broker:** Brokers who trade through exchange provided terminals such as NSE's NEAT, BSE's BOLT, MCX-SX's TWS, etc. (ToR attached as Annexure 1);<sup>55</sup>
  - b. **Type II Broker:** Brokers who trade through API based trading terminals like [CTCL or IML] or IBT/DMA/STWT or SOR facility and who may also be TYPE I Brokers. (ToR attached as Annexure 2)
  - c. **Type III Broker:** Brokers who use Algorithmic Trading facility to trade and who may also be TYPE II Brokers. (ToR attached as Annexure 3)
3. Stock brokers shall select auditors as per the selection norms provided in the guidelines and directions issued by stock exchanges and SEBI from time to time. The Auditor may perform a maximum of 3 successive audits of the stock broker.
4. The stock exchanges shall periodically review ToR of such system audit and, if required, shall suitably revise the ToR after taking into consideration developments that have taken place in the securities market since the last review of ToR, observations reported

---

<sup>54</sup> or other similar trading facilities

<sup>55</sup> Vide Letter MRD/DMS/OW/9500/2015 dated March 31, 2015, SEBI informed Stock Exchanges that System Audit requirement for Type I brokers may be kept on hold till further communication from SEBI.

in the audit reports of the stock brokers and directions issued by SEBI from time to time in this regard.

5. The auditor in its report shall specify compliance / non-compliance status with regard to areas mentioned in ToR. Observations on minor / major deviations as well as qualitative comments for scope for improvement shall also be specified in the report. The auditor shall also take into consideration the observations / issues mentioned in the previous audit reports and cover open items in the report. The audit report submitted by the auditor should be forwarded to the stock exchange by the Stock Broker along with management comments, within 1 month of submission of report by the auditor.
6. Stock exchange shall ensure that the management of the stock broker provides their comment about the non-compliance / non-conformities (NCs) and observations mentioned in the report. For each NC, specific time-bound (within 3 months of submission of report by the exchange) corrective action must be taken and reported to the stock exchange. The auditor should indicate if a follow-on audit is required to review the status of NCs.
7. In order to ensure that the corrective actions are taken by the stock broker, follow-on audit, if any, shall be scheduled by the stock broker within 6 months of submission of the audit report by the system auditor.
8. The system auditors should follow the reporting standard as specified in Annexure 4 of this Framework for the executive summary of the System Audit report to highlight the major findings of the System Audit.

### **Auditor Selection Norms**

1. The Auditor shall have minimum 3 years of experience in IT audit of securities market participants e.g. stock exchanges, clearing corporations, depositories, stock brokers, depository participants etc. The audit experience should cover all the major areas mentioned under Terms of Reference (ToR) of the system audit specified by SEBI / stock exchange.
2. It is recommended that resources employed shall have relevant industry recognized certifications e.g. D.I.S.A. (ICAI) Qualification, CISA (Certified Information System Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium, commonly known as (ISC).
3. The Auditor should have experience of IT audit/governance frameworks and processes conforming to industry leading practices like CobiT.
4. The Auditor shall not have any conflict of interest in conducting fair, objective and independent audit of the Stock Broker. Further, the directors / partners of Auditor firm

shall not be related to any stock broker including its directors or promoters either directly or indirectly.

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

**Terms of Reference (ToR) for Type I Broker**

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

**1. System controls and capabilities**

- a. **Order Tracking** - The system auditor should verify system process and controls at exchange provided terminals with regard to order entry, capturing of IP address of order entry terminals, modification / deletion of orders, status of the current order/outstanding orders and trade confirmation.
- b. **Order Status/ Capture** - Whether the system has capability to generate / capture order id, time stamping, order type, scrip details, action, quantity, price and validity etc.
- c. **Rejection of orders** - Whether system has capability to reject orders which do not go through order level validation at the end of the stock broker and at the servers of respective stock exchanges.
- d. **Communication of Trade Confirmation / Order Status** - Whether the system has capability to timely communicate to Client regarding the Acceptance/ Rejection of an Order / Trade via various media including e-mail; facility of viewing trade log.
- e. **Client ID Verification** - Whether the system has capability to recognize only authorized Client Orders and mapping of Specific user Ids to specific predefined location for proprietary orders.

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

- a. **Online risk management capability** - The system auditor should check whether the system of online risk management (including upfront real-time risk management) is in place for all orders placed through exchange provided terminals.
- b. **Trading Limits** -Whether a system of pre-defined limits / checks such as Order Quantity and Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order Limit, Order Price limit, etc) are in place and only such orders which are within the parameters specified by the RMS are allowed to be pushed into exchange trading engines. The system auditor should check that no user or branch in the system is having unlimited limits on the above parameters.
- c. **Order Alerts and Reports** -Whether the system has capability to generate alerts when orders that are placed are above the limits and has capability to generate reports relating to Margin Requirements, payments and delivery obligations.
- d. **Order Review** -Whether the system has capability to facilitate review of such orders were not validated by the system.

- e. **Back testing for effectiveness of RMS** - Whether the system has capability to identify trades which have exceeded the pre-defined limits (Order Quantity and Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order Limit, Order Price limit) and also exceed corresponding margin availability of clients. Whether deviations from such pre-defined limits are captured by the system, documented and corrective steps taken.
  - f. **Log Management** - Whether the system maintains logs of alerts / changes / deletion / activation / deactivation of client codes and logs of changes to the risk management parameters mentioned above. Whether the system allows only authorized users to set the risk parameter in the RMS.
3. **Password Security**
- a. **Organization Access Policy** - Whether the organization has a well-documented policy that provides for a password policy as well as access control policy for the exchange provided terminals.
  - b. **Authentication Capability** - Whether the system authenticates user credentials by means of a password before allowing the user to login, and whether there is a system for authentication of orders originating from Internet Protocol by means of two-factor authentication, including Public Key Infrastructure (PKI) based implementation of digital signatures.
  - c. **Password Best Practices** - Whether there is a system provision for masking of password, system prompt to change default password on first login, disablement of user id on entering multiple wrong passwords (as defined in the password policy document), periodic password change mandate and appropriate prompt to user, strong parameters for password, deactivation of dormant user id, etc.
4. **Session Management**
- a. **Session Authentication** - Whether the system has provision for Confidentiality, Integrity and Availability (CIA) of the session and the data transmitted during the session by means of appropriate user and session authentication mechanisms like SSL etc.
  - b. **Session Security** - Whether there is availability of an end-to-end encryption for all data exchanged between client and broker systems. or other means of ensuring session security
  - c. **Inactive Session** - Whether the system allows for automatic trading session logout after a system defined period of inactivity.
  - d. **Log Management** - Whether the system generates and maintain logs of Number of users, activity logs, system logs, Number of active clients.
5. **Network Integrity**
- a. **Seamless connectivity** - Whether stock broker has ensured that a backup network link is available in case of primary link failure with the exchange.

- b. **Network Architecture** - Whether the web server is separate from the Application and Database Server.
  - c. **Firewall Configuration** - Whether appropriate firewall is present between stock broker's trading setup and various communication links to the exchange. Whether the firewall is appropriately configured to ensure maximum security.
6. **Access Controls**
- a. **Access to server rooms** - Whether adequate controls are in place for access to server rooms and proper audit trails are maintained for the same.
  - b. **Additional Access controls** - Whether the system provides for any authentication mechanism to access to various components of the exchange provided terminals. Whether additional password requirements are set for critical features of the system. Whether the access control is adequate.
7. **Backup and Recovery**
- a. **Backup and Recovery Policy** - Whether the organization has a well-documented policy on periodic backup of data generated from the broking operations.
  - b. **Log generation and data consistency** - Whether backup logs are maintained and backup data is tested for consistency.
  - c. **System Redundancy** - Whether there are appropriate backups in case of failures of any critical system components.
8. **BCP/DR (Only applicable for Stock Brokers having BCP / DR site)**
- a. **BCP / DR Policy** - Whether the stock broker has a well-documented BCP/ DR policy and plan. The system auditor should comment on the documented incident response procedures.
  - b. **Alternate channel of communication** - Whether the stock broker has provided its clients with alternate means of communication including channel for communication in case of a disaster. Whether the alternate channel is capable of authenticating the user after asking for additional details or OTP (One-Time-Password).
  - c. **High Availability** - Whether BCP / DR systems and network connectivity provide high availability and have no single point of failure for any critical operations as identified by the BCP/DR policy.
  - d. **Connectivity with other FMIs** - The system auditor should check whether there is an alternative medium to communicate with Stock Exchanges and other FMIs.
9. **Segregation of Data and Processing facilities** - The system auditor should check and comment on the segregation of data and processing facilities at the Stock Broker in case the stock broker is also running other business.
10. **Back office data**
- a. **Data consistency** - The system auditor should verify whether aggregate client code data available at the back office of broker matches with the data submitted /

available with the stock exchanges through online data view / download provided by exchanges to members.

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

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

- a. **IT Governance and Policy** - The system auditor should verify whether the relevant IT Infrastructure-related policies and standards exist and are regularly reviewed and updated. Compliance with these policies is periodically assessed.
- b. **IT Infrastructure Planning** - The system auditor should verify whether the plans/policy for the appropriate management and replacement of aging IT infrastructure components have been documented, approved, and implemented. The activities, schedules and resources needed to achieve objectives related to IT infrastructure have been integrated into business plans and budgets.
- c. **IT Infrastructure Availability (SLA Parameters)** - The system auditor should verify whether the broking firm has a process in place to define its required availability of the IT infrastructure, and its tolerance to outages. In cases where there is huge reliance on vendors for the provision of IT services to the brokerage firm the system auditor should also verify that the mean time to recovery (MTTR) mentioned in the Service Level Agreement (SLA) by the service provider satisfies the requirements of the broking firm.
- d. **IT Performance Monitoring (SLA Monitoring)** - The system auditor should verify that the results of SLA performance monitoring are documented and are reported to the management of the broker.

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

**ToR for Type II Broker**

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

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

- a. **Order Tracking** - The system auditor should verify system process and controls at CTCL / IML terminals and CTCL/ IML servers covering order entry, capturing of IP address of order entry terminals, modification / deletion of orders, status of current order/outstanding orders and trade confirmation.
- b. **Order Status/ Capture** - Whether the system has capability to generate / capture order id, time stamping, order type, scrip details, action, quantity, price and validity, etc.
- c. **Rejection of orders** - Whether system has capability to reject orders which do not go through order level validation at CTCL servers and at the servers of respective stock exchanges.
- d. **Communication of Trade Confirmation / Order Status** - Whether the system has capability to timely communicate to Client regarding the Acceptance/ Rejection of an Order / Trade via various media including e-mail; facility of viewing trade log.
- e. **Client ID Verification** - Whether the system has capability to recognize only authorized Client Orders and mapping of Specific user Ids to specific predefined location for proprietary orders.
- f. **Order type distinguishing capability** - Whether system has capability to distinguish the orders originating from (CTCL or IML) / IBT/ DMA / STWT.

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

- a. Processing / approval methodology of new feature request or patches
- b. Fault reporting / tracking mechanism and process for resolution
- c. Testing of new releases / patches / modified software / bug fixes
- d. Version control- History, Change Management process, approval etc.
- e. Development / Test / Production environment segregation.
- f. New release in production - promotion, release note approvals
- g. Production issues / disruptions reported during last year, reasons for such disruptions and corrective actions taken.
- h. User Awareness

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

### 3. Risk Management System (RMS)

- a. **Online risk management capability** - The system auditor should check whether system of online risk management including upfront real-time risk management, is in place for all orders placed through (CTCL or IML) / IBT / DMA / STWT.
- b. **Trading Limits** - Whether a system of pre-defined limits /checks such as Order Quantity and Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order Limit, Order Price limit, etc., are in place and only such orders which are within the parameters specified by the RMS are allowed to be pushed into exchange trading engines. The system auditor should check that no user or branch in the system is having unlimited limits on the above parameters.
- c. **Order Alerts and Reports** - Whether the system has capability to generate alerts when orders that are placed are above the limits and has capability to generate reports relating to margin requirements, payments and delivery obligations.
- d. **Order Review** - Whether the system has capability to facilitate review of such orders that were not validated by the system.
- e. **Back testing for effectiveness of RMS** - Whether system has capability to identify trades which have exceeded the pre-defined limits (Order Quantity and Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order Limit, Order Price limit) and also exceed corresponding margin availability of clients. Whether deviations from such pre-defined limits are captured by the system, documented and corrective steps taken.
- f. **Log Management** - Whether the system maintains logs of alerts / changes / deletion / activation / deactivation of client codes and logs of changes to the risk management parameters mentioned above. Whether the system allows only authorized users to set the risk parameter in the RMS.

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

- a. **Best Execution Policy** - System adheres to the Best Execution Policy while routing the orders to the exchange.
- b. **Destination Neutral** - The system routes orders to the recognized stock exchanges in a neutral manner.
- c. **Class Neutral** - The system provides for SOR for all classes of investors.
- d. **Confidentiality** - The system does not release orders to venues other than the recognized stock Exchange.
- e. **Opt-out** - The system provides functionality to the client who has availed of the SOR facility, to specify for individual orders for which the clients do not want to route order using SOR.

- f. **Time stamped market information** - The system is capable of receiving time stamped market prices from recognized stock Exchanges from which the member is authorized to avail SOR facility.
  - g. **Audit Trail** - Audit trail for SOR should capture order details, trades and data points used as a basis for routing decision.
  - h. **Server Location** - The system auditor should check whether the order routing server is located in India.
  - i. **Alternate Mode** - The system auditor should check whether an alternative mode of trading is available in case of failure of SOR Facility
5. **Password Security**
- a. **Organization Access Policy** - Whether organization has a well-documented policy that provides for a password policy as well as access control policy for exchange provided terminals and for API based terminals.
  - b. **Authentication Capability** - Whether the system authenticates user credentials by means of a password before allowing the user to login, and whether there is a system for authentication of orders originating from Internet Protocol by means of two-factor authentication, including Public Key Infrastructure (PKI) based implementation of digital signatures.
  - c. **Password Best Practices** - Whether there is a system provision for masking of password, system prompt to change default password on first login, disablement of user id on entering multiple wrong passwords (as defined in the password policy document), periodic password change mandate and appropriate prompt to user, strong parameters for password, deactivation of dormant user id, etc.
6. **Session Management**
- a. **Session Authentication** - Whether system has provision for Confidentiality, Integrity and Availability (CIA) of the session and the data transmitted during the session by means of appropriate user and session authentication mechanisms like SSL etc.
  - b. **Session Security** - Whether there is availability of an end-to-end encryption for all data exchanged between client and broker systems or other means of ensuring session security. Whether session login details are stored on the devices used for IBT and STWT.
  - c. **Inactive Session** - Whether the system allows for automatic trading session logout after a system defined period of inactivity.
  - d. **Log Management** - Whether the system generates and maintains logs of Number of users, activity logs, system logs, Number of active clients.
7. **Database Security**
- a. **Access** - Whether the system allows CTCL or IML database access only to authorized users / applications.

- b. **Controls** - Whether the CTCL or IML database server is hosted on a secure platform, with Username and password stored in an encrypted form using strong encryption algorithms.
8. **Network Integrity**
- a. **Seamless connectivity** - Whether the stock broker has ensured that a backup network link is available in case of primary link failure with the exchange.
  - b. **Network Architecture** - Whether the web server is separate from the Application and Database Server.
  - c. **Firewall Configuration** - Whether appropriate firewall is present between stock broker's trading setup and various communication links to the exchange. Whether the firewall is appropriately configured to ensure maximum security.
9. **Access Controls**
- a. **Access to server rooms** - Whether adequate controls are in place for access to server rooms and proper audit trails are maintained for the same.
  - b. **Additional Access controls** - Whether the system provides for two factor authentication mechanism to access to various CTCL or IML components. Whether additional password requirements are set for critical features of the system. Whether the access control is adequate.
10. **Backup and Recovery**
- a. **Backup and Recovery Policy** - Whether the organization has a well-documented policy on periodic backup of data generated from the broking operations.
  - b. **Log generation and data consistency** - Whether backup logs are maintained and backup data is tested for consistency
  - c. **System Redundancy** - Whether there are appropriate backups in case of failures of any critical system components
11. **BCP/DR** (Only applicable for Stock Brokers having BCP / DR site)
- a. **BCP / DR Policy** - Whether the stock broker has a well-documented BCP/ DR policy and plan. The system auditor should comment on the documented incident response procedures.
  - b. **Alternate channel of communication** - Whether the stock broker has provided its clients with alternate means of communication including channel for communication in case of a disaster. Whether the alternate channel is capable of authenticating the user after asking for additional details or OTP (One-Time-Password).
  - c. **High Availability** - Whether BCP / DR systems and network connectivity provide high availability and have no single point of failure for any critical operations as identified by the BCP/ DR policy.
  - d. **Connectivity with other FMIs** - The system auditor should check whether there is an alternative medium to communicate with Stock Exchanges and other FMIs.

12. **Segregation of Data and Processing facilities** - The system auditor should check and comment on the segregation of data and processing facilities at the Stock Broker in case the stock broker is also running other business.

13. **Back office data**

- a. **Data consistency** - The system auditor should verify whether aggregate client code data available at the back office of broker matches with the data submitted / available with the stock exchanges through online data view / download provided by exchanges to members.
- b. **Trail Logs** - The system auditor should specifically comment on the logs of Client Code data to ascertain whether editing or deletion of records have been properly documented and recorded and does not result in any irregularities.

14. **User Management**

- a. **User Management Policy** - The system auditor should check whether the stock broker has a well-documented policy that provides for user management and the user management policy explicitly defines user, database and application Access Matrix.
- b. **Access to Authorized users** - The system auditor should check whether the system allows access only to the authorized users of the CTCL or IML System. Whether there is a proper documentation of the authorized users in the form of User Application approval, copies of User Qualification and other necessary documents.
- c. **User Creation / Deletion** - The system auditor should check whether new users' ids were created / deleted as per CTCL or IML guidelines of the exchanges and whether the user ids are unique in nature.
- d. **User Disablement** - The system auditor should check whether non-complaint users are disabled and appropriate logs (such as event log and trade logs of the user) are maintained.

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

- a. **IT Governance and Policy** - The system auditor should verify whether the relevant IT Infrastructure-related policies and standards exist and are regularly reviewed and updated. Compliance with these policies is periodically assessed.
- b. **IT Infrastructure Planning** - The system auditor should verify whether the plans/policy for the appropriate management and replacement of aging IT infrastructure components have been documented, approved, and implemented. The activities, schedules and resources needed to achieve objectives related to IT infrastructure have been integrated into business plans and budgets.

- c. **IT Infrastructure Availability (SLA Parameters)** - The system auditor should verify whether the broking firm has a process in place to define its required availability of the IT infrastructure, and its tolerance to outages. In cases where there is huge reliance on vendors for the provision of IT services to the brokerage firm the system auditor should also verify that the mean time to recovery (MTTR) mentioned in the Service Level Agreement (SLA) by the service provider satisfies the requirements of the broking firm.
  - d. **IT Performance Monitoring (SLA Monitoring)** - The system auditor should verify that the results of SLA performance monitoring are documented and are reported to the management of the broker.
16. **Exchange specific exceptional reports** - The additional checks recommended by a particular exchange need to be looked into and commented upon by the System Auditor over and above the ToR of the System audit.
17. **Software Testing Procedures** - The system auditor should check whether the stock broker has complied with the guidelines and instructions of SEBI / stock exchanges with regard to testing of software and new patches, including the following:
- a. **Test Procedure Review** - The system auditor should evaluate whether the procedures for system and software testing were proper and adequate.
  - b. **Documentation** - The system auditor should verify whether the documentation related to testing procedures, test data, and resulting output were adequate and follow the organization's standards.
  - c. **Test Cases** - The system auditor should review the internal test cases and comment upon the adequacy of the same with respect to the requirements of the Stock Exchange and SEBI.

**ToR for Type III Broker**

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

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

- a. **Order Tracking** - The system auditor should verify system process and controls at CTCL / IML terminals and CTCL/ IML servers covering order entry, capturing IP address of order entry, modification / deletion of orders, status of current order/outstanding orders and trade confirmation.
- b. **Order Status/ Capture** - Whether the system has capability to generate / capture order id, time stamping, order type, scrip details, action, quantity, price and validity etc.
- c. **Rejection of orders** - Whether the system has capability to reject orders which do not go through order level validation at CTCL servers and at the servers of respective exchanges.
- d. **Communication of Trade Confirmation / Order Status** - Whether the system has capability to timely communicate to client regarding the Acceptance/ Rejection of an Order / Trade via various media including e-mail; facility of viewing trade log.
- e. **Client ID Verification** - Whether the system has capability to recognize only authorized Client Orders and mapping of Specific user Ids to specific predefined location for proprietary orders.
- f. **Order type distinguishing capability** - Whether the system has capability to distinguish the orders originating from (CTCL or IML) / IBT / DMA / STWT / SOR / Algorithmic Trading.

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

- a. Processing/approval methodology of new feature request or patches
- b. Fault reporting / tracking mechanism and process for resolution
- c. Testing of new releases / patches / bug fixes
- d. Version control- History, Change Management process, approval etc.
- e. Development / Test/ Production environment segregation.
- f. New release in production - promotion, release note approvals
- g. Production issues/ disruptions reported during last year, reasons for such disruptions and corrective actions taken.
- h. User Awareness

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

### 3. Risk Management System (RMS)

- a. **Online risk management capability** - The system auditor should check whether the online risk management including upfront real-time risk management, is in place for all orders placed through (CTCL or IML) / IBT/ DMA / SOR / STWT / Algorithmic Trading.
- b. **Trading Limits** - Whether a system of pre-defined limits / checks such as Order Quantity and Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order Limit, Order Price limit, etc., are in place and only such orders which are within the parameters specified by the RMS are allowed to be pushed into exchange trading engines. The system auditor should check that no user or branch in the system is having unlimited limits on the above parameters.
- c. **Order Alerts and Reports** - Whether the system has capability to generate alerts when orders that are placed are above the limits and has capability to generate reports relating to margin requirements, payments and delivery obligations.
- d. **Order Review** - Whether the system has capability to facilitate review of such orders that were not validated by the system.
- e. **Back testing for effectiveness of RMS** - Whether the system has capability to identify trades which have exceeded the pre-defined limits (Order Quantity and Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order Limit, Order Price limit) and also exceed corresponding margin availability of clients. Whether deviations from such pre-defined limits should be captured by the system, documented and corrective steps taken.
- f. **Log Management** - Whether the system maintains logs of alerts / changes / deletion / activation / deactivation of client codes and logs of changes to the risk management parameters mentioned above. Whether the system allows only authorized users to set the risk parameter in the RMS.

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

- a. **Best Execution Policy** - System adheres to the Best Execution Policy while routing the orders to the exchange.
- b. **Destination Neutral** - The system routes orders to the recognized stock exchanges in a neutral manner.
- c. **Class Neutral** - The system provides for SOR for all classes of investors.

- d. **Confidentiality** - The system does not release orders to venues other than the recognized stock Exchange.
  - e. **Opt-out** - The system provides functionality to the client who has availed of the SOR facility, to specify for individual orders for which the clients do not want to route order using SOR.
  - f. **Time stamped market information** - The system is capable of receiving time stamped market prices from recognized stock Exchanges from which the member is authorized to avail SOR facility.
  - g. **Audit Trail** - Audit trail for SOR should capture order details, trades and data points used as a basis for routing decision.
  - h. **Server Location** - The system auditor should check whether the order routing server is located in India.
  - i. **Alternate Mode** - The system auditor should check whether an alternative mode of trading is available in case of failure of SOR Facility
5. **Algorithmic Trading** - The system auditor should check whether proper procedures have been followed and proper documentation has been maintained for the following:
- a. **Change Management** -Whether any changes (modification/addition) to the approved algos were informed to and approved by stock exchange. The inclusion / removal of different versions of algos should be well documented.
  - b. **Online Risk Management capability**- The CTCL or IML server should have capacity to monitor orders / trades routed through algo trading and have online risk management for all orders through Algorithmic trading and ensure that Price Check, Quantity Check, Order Value Check, Cumulative Open Order Value Check are in place.
  - c. **Risk Parameters Controls** - The system should allow only authorized users to set the risk parameter. The System should also maintain a log of all the risk parameter changes made.
  - d. **Information / Data Feed** - The auditor should comment on the various sources of information / data for the algo and on the likely impact (run away /loop situation) of the failure one or more sources to provide timely feed to the algorithm. The system auditor should verify that the algo automatically stops further processing in the absence of data feed.
  - e. **Check for preventing loop or runaway situations** - The system auditor should check whether the brokers have real time monitoring systems to identify and shutdown/stop the algorithms which have not behaved as expected.
  - f. **Algo / Co-location facility Sub-letting** - The system auditor should verify if the algo/ co-location facility has not been sub-letted to any other firms to access the exchange platform.

- g. **Audit Trail** - The system auditor should check the following areas in audit trail:
- i. Whether the audit trails can be established using unique identification for all algorithmic orders and comment on the same.
  - ii. Whether the broker maintains logs of all trading activities.
  - iii. Whether the records of control parameters, orders, traders and data emanating from trades executed through algorithmic trading are preserved/maintained by the Stock Broker.
  - iv. Whether changes to the control parameters have been made by authorized users as per the Access Matrix. The system auditor should specifically comment on the reasons and frequency for changing of such control parameters. Further, the system auditor should also comment on the possibility of such tweaking leading to run away/loop situation.
  - v. Whether the system captures the IP address from where the algo orders are originating.
- h. **Systems and Procedures** - The system auditor should check and comment on the procedures, systems and technical capabilities of stock broker for carrying out trading through use of Algorithms. The system auditor should also identify any misuse or unauthorized access to algorithms or the system which runs these algorithms.
- i. **Reporting to Stock Exchanges** - The system auditor should check whether the stock broker is informing the stock exchange regarding any incidents where the algos have not behaved as expected. The system auditor should also comment upon the time taken by the stock broker to inform the stock exchanges regarding such incidents.

## 6. Password Security

- a. **Organization Access Policy** - The system auditor should check whether the stock broker has a well-documented policy that provides for a password policy as well as access control policy for exchange provided terminals and for API based terminals.
- b. **Authentication Capability** - Whether the system authenticates user credentials by means of a password before allowing the user to login. Whether there is a system for authentication of orders originating from Internet Protocol by means of two-factor authentication, including Public Key Infrastructure (PKI) based implementation of digital signatures.
- c. **Password Best Practices** - Whether there is a system should for masking of password, system prompt to change default password on first login, disablement of user id on entering multiple wrong passwords (as defined in the password

policy document), periodic password change mandate and appropriate prompt to user, strong parameters for password, deactivation of dormant user id, etc.

## 7. Session Management

- a. **Session Authentication** - Whether the system has provision for Confidentiality, Integrity and Availability (CIA) of the session and the data transmitted during the session by means of appropriate user and session authentication mechanisms like SSL etc.
- b. **Session Security** - Whether there is availability of an end-to-end encryption for all data exchanged between client and broker system or other means of ensuring session security. Whether session login details are stored on the devices used for IBT and STWT.
- c. **Inactive Session** - Whether the system allows for automatic trading session logout after a system defined period of inactivity.
- d. **Log Management** - Whether the system generates and maintains logs of number of users, activity logs, system logs, number of active clients.

## 8. Database Security

- a. **Access** - Whether the system allows CTCL or IML database access only to authorized users / applications.
- b. **Controls** - Whether the CTCL or IML database server is hosted on a secure platform, with username and password stored in an encrypted form using strong encryption algorithms.

## 9. Network Integrity

- a. **Seamless connectivity** - Whether the stock broker has ensured that a backup network link is available in case of primary link failure with the exchange.
- b. **Network Architecture** - Whether the web server is separate from the Application and Database Server.
- c. **Firewall Configuration** - Whether appropriate firewall are present between the stock broker's trading setup and various communication links to the exchange. Whether the firewalls should be appropriately configured to ensure maximum security.

## 10. Access Controls

- a. **Access to server rooms** - Whether adequate controls are in place for access to server rooms, proper audit trails should be maintained for the same.
- b. **Additional Access controls** - Whether the system should provide for two factor authentication mechanism to access to various CTCL or IML components.

Whether additional password requirements are set for critical features of the system. Whether the access control is adequate.

#### 11. Backup and Recovery

- a. **Backup and Recovery Policy** – Whether the organization has a well-documented policy on periodic backup of data generated from the broking operations.
- b. **Log generation and data consistency** – Whether backup logs are maintained and backup data should be tested for consistency.
- c. **System Redundancy** – Whether there are appropriate backups in case of failures of any critical system components.

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

- a. **BCP / DR Policy** – Whether the stock broker has a well-documented BCP / DR policy and plan. The system auditor should comment on the documented incident response procedures.
- b. **Alternate channel of communication** – Whether the stock broker has provided its clients with alternative means of communication including channel for communication in case of a disaster. Whether the alternate channel is capable of authenticating the user after asking for additional details or OTP (One-Time-Password).
- c. **High Availability** – Whether BCP / DR systems and network connectivity provide high availability and have no single point of failure for any critical operations as identified by the BCP / DR policy.
- d. **Connectivity with other FMIs** – The system auditor should check whether there is an alternative medium to communicate with Stock Exchanges and other FMIs.

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

#### 14. Back office data

- a. **Data consistency** – The system auditor should verify whether aggregate client code data available at the back office of broker matches with the data submitted / available with the stock exchanges through online data view / download provided by exchanges to members.
- b. **Trail Logs** – The system auditor should specifically comment on the logs of Client Code data to ascertain whether editing or deletion of records have been properly documented and recorded and does not result in any irregularities.

## 15. User Management

- a. **User Management Policy** - The system auditor should verify whether the stock broker has a well-documented policy that provides for user management and the user management policy explicitly defines user, database and application access matrix.
- b. **Access to Authorized users** - The system auditor should verify whether the system allows access only to the authorized users of the CTCL or IML system. Whether there is a proper documentation of the authorized users in the form of user application approval, copies of user qualification and other necessary documents.
- c. **User Creation / Deletion** - The system auditor should verify whether new user's ids should be created / deleted as per CTCL or IML guidelines of the exchanges and whether the user ids are unique in nature.
- d. **User Disablement** - The system auditor should verify whether non-complaint users are disabled and appropriate logs such as event log and trade logs of the user should be maintained

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

- a. **IT Governance and Policy** - The system auditor should verify whether the relevant IT Infrastructure-related policies and standards exist and are regularly reviewed and updated. Compliance with these policies is periodically assessed.
- b. **IT Infrastructure Planning** - The system auditor should verify whether the plans/policy for the appropriate management and replacement of aging IT infrastructure components have been documented, approved, and implemented. The activities, schedules and resources needed to achieve objectives related to IT infrastructure have been integrated into business plans and budgets.
- c. **IT Infrastructure Availability (SLA Parameters)** - The system auditor should verify whether the broking firm has a process in place to define its required availability of the IT infrastructure, and its tolerance to outages. In cases where there is huge reliance on vendors for the provision of IT services to the brokerage firm the system auditor should also verify that the mean time to recovery (MTTR) mentioned in the Service Level Agreement (SLA) by the service provider satisfies the requirements of the broking firm.
- d. **IT Performance Monitoring (SLA Monitoring)** - The system auditor should verify that the results of SLA performance monitoring are documented and are reported to the management of the broker.

- 17. Exchange specific exceptional reports** - The additional checks recommended by a particular exchange need to be looked into and commented upon by the system auditor over and above the ToR of the system audit.
- 18. Software Testing Procedures** - The system auditor shall audit whether the stock broker has complied with the guidelines and instructions of SEBI / stock exchanges with regard to testing of software and new patches including the following:
- a. **Test Procedure Review** - The system auditor should review and evaluate the procedures for system and program testing. The system auditor should also review the adequacy of tests.
  - b. **Documentation** - The system auditor should review documented testing procedures, test data, and resulting output to determine if they are comprehensive and if they follow the organization's standards.
  - c. **Test Cases** - The system auditor should review the test cases and comment upon the adequacy of the same with respect to the requirements of the Stock Exchange and various SEBI Circulars.

**Executive Summary Reporting Format**
**I. For Preliminary Audit**

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

**Description of relevant Table heads**

- Audit Date** - This indicates the date of conducting the audit.
- 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.*)
- Status/ Nature of Findings** - the category can be specified for example:
  - Non-Compliant
  - Work in progress
  - Observation
  - Suggestion
- Risk Rating of Findings** - A rating has to be 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
<b>HIGH</b>	Weakness in control those represent exposure to the organization or risks that could lead to instances of noncompliance with the requirements of TORs. These risks need to be addressed with utmost priority.
<b>MEDIUM</b>	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.
<b>LOW</b>	Potential weaknesses in controls, which in combination with other weakness can develop into an exposure. Suggested improvements for situations not immediately/ directly affecting controls.

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

## II. For Follow on/ Follow up System Audit

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

### Description of relevant Table heads

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

## Annexure IXA

### System Audit Framework

#### Audit Process

1. For the System Audit, the following broad areas shall be considered in order to ensure that the audit is comprehensive and effective:
  - a. The Audit shall be conducted according to the Norms, Terms of Reference (TOR) and Guidelines issued by SEBI/Clearing Corporations(CCs). Professional Clearing Members(PCMs) shall select the Auditors based on the prescribed Auditor Selection Norms and TOR. The Governing Board of the PCMs shall approve the appointment of the Auditors.
  - b. An Auditor can perform a maximum of 3 successive audits. However, such auditor shall be eligible for re-appointment after a cooling-off period of two years.
  - c. Further, during the cooling-off period, the incoming auditor may not include:
    - i. Any firm that has common partner(s) with the outgoing audit firm; and
    - ii. Any associate / affiliate firm(s) of the outgoing audit firm which are under the same network of audit firms wherein the term "same network" includes the firms operating or functioning, hitherto or in future, under the same brand name, trade name or common control.
  - d. The number of years an auditor has performed an audit prior to this circular shall also be considered in order to determine its eligibility in terms of sub-clauses b and c above.
  - e. The scope of the Audit may be broadened by the Auditor to inter-alia incorporate any new developments that may arise due to issuance of circulars/ directions/ advice by SEBI/Clearing Corporation from time to time.
  - f. The audit shall be conducted for each financial year. Further, the audit shall be completed within 2 months from the end of the audit period. The Audit report shall be submitted to CCs within one month of completion of the Audit, after approval of the Governing Board (or equivalent governance structure as applicable to the entity). PCMs, who have conducted clearing activities during the audit period are liable for submission of the System Audit report.

- g. In the Audit report, the Auditor shall include its comments on whether the areas covered in the Audit are in compliance with the norms/ directions/ advices issued by SEBI, Clearing Corporation, internal policy of the PCM, etc. Further, the Audit report shall also include specific non-compliances (NCs), observations for minor deviations and suggestions for improvement. The audit report shall take previous audit reports into consideration and cover any open items therein. The Auditor should indicate if a follow-on audit is required to review the status of NCs.
- h. For each of the NCs/ observations and suggestions made by the Auditor, specific corrective action as deemed fit may be taken by the PCM. The management of the PCM shall provide its comments on the NCs, observations and suggestions made by the Auditor, corrective actions taken or proposed to be taken along with time-line for such corrective actions.
- i. The Audit report along with the comments of management shall be placed before the Governing Board (or equivalent governance structure as applicable to the entity) of the PCM. The Audit report along with comments of the Governing Board shall be submitted to Clearing Corporation, within one month of completion of audit.
- j. The follow-on audit should be completed within one month of the corrective actions taken by the PCM. After the follow-on audit, the PCM shall submit a report to CC within one month from the date of completion of the follow-on audit. The report shall include updated Issue-Log to indicate the corrective actions taken and specific comments of the Auditor on the NCs and the corrective actions.
- k. In cases wherein follow-on audit is not required, the PCM shall submit an Action Taken Report (ATR) to the Auditor. After verification of the ATR by the Auditor, the PCM shall submit a report to Clearing Corporation within one month from the date of completion of verification by the Auditor. The report shall include updated Issue-Log to indicate the corrective actions taken and specific comments of the auditor on the ATR.
- l. The overall timeline from the last date of the audit period till completion of final compliance by PCM, including follow-on audit, if any, should not exceed 6 months. In exceptional cases, if PCM is of the view that compliance with certain observations may extend beyond said period, then the concerned PCM shall seek specific approval from the Governing Board.
- m. The auditee team, who is responsible for direct liaison with the system auditor, at least one of the members must have thorough knowledge and experience in handling system audit.

## Auditor Selection Norms

2. PCMs shall ensure compliance with the following norms while appointing Auditor:
  - a. Lead Auditor must have minimum 3 years of demonstrable experience in IT audit of securities market participants e.g. stock brokers, clearing members, exchanges, clearing corporations, depositories, intermediaries, etc. and/ or financial services sector i.e. banking, insurance, Fin-tech etc.
  - b. The team performing system audit must have experience in / direct access to experienced resources in the areas covered under TOR. It is recommended that resources deployed by the Auditor for the purpose of system audit shall have relevant industry recognized certifications e.g. CISA (Certified Information Systems Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, GSNA (GIAC Systems and Network Auditor), CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium, commonly known as (ISC).
  - c. The Auditor shall have experience in working on Network audit/IT audit/governance/IT service management frameworks and processes conforming to industry leading practices like CobiT/ ISO 27001 and beyond.
  - d. The Auditor should have the capability to undertake forensic audit and undertake such audit as part of system audit, if required.
  - e. The Auditor must not have any conflict of interest in conducting fair, objective and independent audit of the PCM. It should not have been engaged over the last three years in any consulting engagement with any departments / units of the entity being audited.
  - f. The Auditor should not have any cases pending against it, which point to its incompetence and/or unsuitability to perform the audit task.
  - g. The proposed audit agency must be empanelled with CERT-In on the date of appointment as auditor and date of submission of audit report.
  - h. Any criteria, in addition to the aforesaid criteria, that the PCM may deem fit for the purpose of selection of Auditor.

### Audit Report Guidelines

3. The Audit report should cover each of the major areas mentioned in the TOR and compliance with SEBI and CC circulars/directions/advice, etc. related to technology. The Auditor in the Audit report shall give its views indicating the NCs to the standards or observations or suggestions. For each section, auditors should also provide qualitative inputs/suggestions about ways to improve the processes, based upon the best industry practices.
4. The report should also include tabulated data to show NCs / observations for each of the major areas in the TOR.
5. The audit report to include point-wise compliance of areas prescribed in TOR and areas emanating from relevant SEBI and CC circulars/directions/advice along with any accompanying evidence.
6. Evidences should be specified in the audit report while reporting/ closing an issue.
7. A detailed report with regard to the system audit shall be submitted to CC. The report shall include an Executive Summary as per the following format:

Issue	Description	Responsibility
Major Area	Comprehensive identification of major areas in compliance with various SEBI & Clearing Corporation circulars /	Auditor/Auditee

	norms and internal policies of PCM	
<b>Point wise Compliance</b>	Point-wise list of areas/relevant clauses in TOR against which compliance is being audited (in tabular format).	Auditor
<b>Description of Finding/ Observation</b>	Describe the findings in sufficient detail, referencing any accompanying evidence (e.g. procedure manual, interview notes, reports etc.)	Auditor
<b>Reference</b>	Reference to the section in detailed report - where full background information about the findings are available	Auditor
<b>Process/ Unit</b>	Process or unit where the audit is conducted and the finding pertains to	Auditor
<b>Category of Findings</b>	Major/Minor Non-compliance, Observation, Suggestion etc.	Auditor

\*\*\*\*\*

## Annexure IXB

### System Audit Program – Terms of Reference (TOR)

1. The scope of audit shall encompass all the IT resources including hardware, software, network, policies, procedures etc. of PCMs (Primary Data Centre (PDC), Disaster Recovery Site (DRS) and Near Site (NS), if applicable).

#### 2. IT environment

##### 2.1. Organization details

- a. Name
- b. Address
- c. IT team size (in house- employees)
- d. IT team size (vendors)

##### 2.2. IT and network set up and usage

- a. PDC, DRS, NS and Regional/ Branch offices (location, owned/ outsourced), if applicable
- b. Connectivity amongst PDC, NS and DRS, if applicable
- c. IT infrastructure / applications pertaining to the activities done as a PCM.
- d. System Architecture
- e. Network architecture
- f. Telecommunication network

#### 3. IT Governance

##### 3.1. Whether IT Governance framework exists to include the following:

- a. IT organization structure including roles and responsibilities of key IT personnel;
- b. IT governance processes including policy making, implementation and monitoring to ensure that the governance principles are followed;

##### 3.2. IT policies and procedures

- a. Whether the organization has a defined and documented IT policy. If yes, is it approved by the Governing Board (GB)?
- b. Is the current System Architecture, including infrastructure, network

and application components describing system linkages and dependencies, documented?

c. Whether defined and documented Standard Operating Procedures (SOPs)/Policy for the following processes are in place.

- i. IT Assets Acquisition
- ii. Access Management
- iii. Change Management
- iv. Backup and Recovery
- v. Incident Management
- vi. Problem Management
- vii. Patch Management
- viii. Data Centre Operations
- ix. Operating Systems and Database Management
- x. Network Management
- xi. DRS Operations
- xii. Data Retention and Disposal
- xiii. Asset Inventory
- xiv. Database security
- xv. Password Security
- xvi. Archived and backed up data security

3.3. Whether the above mentioned SOPs/Policies are reviewed at periodic intervals or upon the occurrence of any major event.

3.4. In this regard, whether any organization policy has been formulated by the PCM.

#### **4. Business Controls**

##### **4.1. General Controls for Data Centre Facilities**

- a. Application Access – segregation of duties, database and application access etc. (Approved Policy clearly defining roles and responsibilities of the personnel handling business operations)
- b. Maintenance Access – vendor engineers
- c. Physical Access controls – permissions, logging, exception reporting &

alerts

- d. Environmental Controls – fire protection, AC monitoring, etc.
- e. Fault Resolution Mechanism
- f. Folder Sharing and Back Up Controls – safeguard of critical information on local desktops
- g. Incidences of violations in the previous audit report and corrective action(s), if any, taken
- h. Any other controls, as deemed fit, by the PCM

#### 4.2. Risk Management System (RMS)

- a. Risk management capability – The system auditor should check whether system of risk management including upfront real-time risk management if applicable is in place.
- b. 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 exceeded corresponding margin availability of clients. Whether deviations from such pre-defined limits are captured by the system, documented and corrective steps taken.
- c. Log Management – Whether the system maintains logs of alerts / changes / deletion / activation / deactivation of client codes and logs of changes to the risk management parameters mentioned above. Whether the system allows only authorized users to set the risk parameter in the RMS.

#### 4.3. Software change control

- a. Whether pre-implementation review of application controls (including controls over change management) was undertaken.
- b. Adherence to secure Software Development Life Cycle (SDLC) / Software Testing Life Cycle (STLC) standards/ methodologies
- c. Whether post implementation review of application controls was

undertaken.

- d. Is the review of processes to ensure data integrity post implementation of new application or system followed by implementation team?
- e. User awareness
- f. Processing of new feature request
- g. Fault reporting / tracking mechanism & process for resolutions
- h. Testing of New releases / Bug-fixes - Testing process (automation level)
- i. Version Control - History, Change Management process etc.
- j. Development / Test/ Production environment - Segregation
- k. New Release in Production - Promotion, Release note approvals
- l. Production Issues / disruptions reported in the previous audit report, root cause analysis & corrective actions taken, if any
- m. Software Development Stage
- n. Software Design to ensure adequate system capacity to enable functioning in a degraded manner in the event of a crash.
- o. Software Testing framework, methodology and process guideline
- p. Any other controls, as deemed fit, by the PCM

#### 4.4. Data Communication/ Network Controls

- a. Network Administration - Link, Path, Redundancy, No single point of failure, high availability, fault tolerance, Monitoring, breakdown resolution etc.
- b. WAN Management - Connectivity provisions for business continuity.
- c. Connection Permissions - Restriction on need to have basis
- d. Incidences of access violations observed in the previous report & corrective actions taken, if any
- e. Any other controls, as deemed fit, by the PCM

#### 4.5. Security Controls

- a. Email Archival Implementation
- b. Anti-virus and malware controls

#### 4.6. Access Policy and Controls

- a. Defined and documented policies and procedures for managing access to applications and infrastructure –PDC, DRS, NS (if applicable) , branches (including network, operating systems and database) and approved by relevant authority
- b. Review of access logs
- c. Access rights and roles review procedures for all systems
- d. Segregation of Duties (SOD) matrix describing key roles
- e. Risk acceptance for violation of SOPs and alternate mechanism put in place
- f. Privileged access to system and record of logs,
- g. Periodic monitoring of access rights for privileged users
- h. Authentication mechanisms used for access to systems including use of passwords, One Time Passwords (OTP), Single Sign on, etc.
- i. BYOD (bring your own device) policies
- j. Any other controls, as deemed fit, by the PCM

#### 4.7. Performance Audit

- a. Review of systems (hardware, software, network) performance over the period
- b. Current system utilization

#### 4.8. Business Continuity / Disaster Recovery Facilities

- a. Business Continuity Planning (BCP) manual, including Business Impact Analysis (BIA), Risk Assessment and Disaster Recovery (DR) process, Roles and responsibilities of Incident Response Team (IRT) /Crisis Management Team (CMT), if applicable, employees, support/outsourced staff.
- b. Implementation of policies
- c. Back-up procedures and recovery mechanism using back-ups.
- d. Storage of Back-up (Remote site, DRS etc.)
- e. Redundancy – Equipment, Network, Site etc.
- f. DRS installation and Drills - Management statement on targeted resumption capability (in terms of time required & extent of loss of data)

- g. Evidence of achieving the set targets during the DR drills in event of various disaster scenarios., if applicable
  - h. Debrief / review of any actual event when the DR/BCP was invoked during the year, if applicable.
  - i. User awareness and training
  - j. Is Recovery Time Objective (RTO) /Recovery Process Objective (RPO) during Business Impact Assessment (BIA) documented, if applicable?
  - k. Is review of BCP-DR undertaken annually or in case of major change in business/ infrastructure?
  - l. Testing of BCP-DR plan through appropriate strategies including simulations, DR drills, system recovery, etc.
- 4.9. IT/Network Support & IT Asset Management
- a. Utilization Monitoring - including report of prior year utilization
  - b. Capacity Planning - including projection of business volumes
  - c. Capacity and performance management process for the network/systems
  - d. IT (S/W, H/W & N/W) Assets, Licenses & maintenance contracts
  - e. Comprehensive review of Assets life cycle management (Acquisition, commissioning, deployment, monitoring, maintenance and de commissioning) and relevant records related to it.
  - f. Insurance
  - g. Disposal of Equipment, media, and other electronic waste as per applicable waste disposal guidelines etc.
- 4.10. Segregation of Data and Processing facilities - The system auditor should check and comment on the segregation of data and processing facilities in case the member is also running other business.
5. Entity Specific Software used for or in support of trading/clearing systems / peripheral systems and critical processes.

## **6. Human Resources Management**

- 6.1. Screening of Employee, Third party vendors / contractors
- 6.2. Onboarding
- 6.3. Offboarding
- 6.4. Consequence Management (Incident / Breach of policies)
- 6.5. Awareness and Trainings
- 6.6. Non-Disclosure Agreements (NDAs) and confidentiality agreement

7. The results of all testing that was conducted before deployment of any IT system/application in production environment, shall be checked by auditor during system audit.

## **8. IT Vendor Selection and Management**

- 8.1. Identification of eligible vendors
- 8.2. Dissemination process of Request for Proposal (RFP)
- 8.3. Definition of criteria of evaluation
- 8.4. Process of competitive analysis
- 8.5. Approach for selection
- 8.6. Escrow arrangement for keeping source code

## **9. E-Mail system**

- 9.1 Existence of policy for the acceptable use of electronic mail
- 9.2 Regulations governing file transfer and exchange of messages with external parties
- 9.3 Rules based on which e-mail addresses are assigned
- 9.4 Storage, backup and retrieval

## **10.Redressal of Technological Complaints**

- 10.1 Ageing analysis of technology complaints
- 10.2 Whether all complaints received are brought to their logical conclusion?

## **11.Any other Item(s)**

- 11.1 Observation(s) based on previous Audit Report (s)
- 11.2 Any new direction/instruction that may be informed by Clearing Corporation and/or SEBI.

**Annexure IXC**

**Format for monitoring compliance with requirements emanating from SEBI and Clearing Corporation (CC) circulars/guidelines/advisories related to technology**

Sl. No.	Date of SEBI/CC circular/directions/advice, etc.	Subject	Technological requirements specified by SEBI/CC in brief	Mechanism put in place by the PCMs	Non compliances with SEBI/CC circulars / directions, etc.	Compliance status (Open/closed)	Comments of the Management	Time-line for taking corrective action in case of open observations

\*\*\*\*\*

**Annexure IXD**

**Exception Observation Reporting Format**

Note: PCMs are expected to submit following information with regard to exceptional major non-compliances (NCs) / minor NCs observed in the System Audit. PCMs should also categorically highlight those observations/NCs/suggestions pointed out in the System Audit (current and previous) which are not yet complied with.

Name of the PCM: \_\_\_\_\_

Name of the Auditor: \_\_\_\_\_

Systems Audit Report Date: \_\_\_\_\_

**Table 1: For preliminary audit**

Audit period	Observation No.	Description of finding	Department of PCM	Status/ Nature of finding	Risk Rating of finding as per Auditor	Audit TOR clause	Root Cause Analysis	Impact Analysis	Corrective Actions proposed by auditor	Deadline for the corrective action	Management response in case of acceptance of associated risks	Whether similar issue was observed in any of the previous 3 Audits

**Description of relevant Table heads**

1. **Audit Period** – This indicates the period of audit

2. **Description of findings/observations** – Description of the findings in sufficient details, referencing any accompanying evidence
3. **Status/ Nature of Findings** – The category can be specified, for example:
  - a. Non-compliant (Major/Minor)
  - b. Work in progress
  - c. Observation
  - d. Suggestion
4. **Risk Rating of finding** - A rating has to be given for each of the observations based on its impact and severity to reflect the risk exposure as well as the suggested priority for action

Rating	Description
<b>HIGH</b>	Represents weakness in control with respect to threat(s) that is /are sufficiently capable and impacts asset (s) leading to regulatory non-compliance, significant financial, operational and reputational loss. These observations need to be addressed with utmost priority.
<b>MEDIUM</b>	Represents weakness in control with respect to threat(s) that is /are sufficiently capable and impacts asset (s) leading to exposure in terms of financial, operational and reputational loss. These observations need to be addressed reasonable timeframe.
<b>LOW</b>	Represents weaknesses in control, 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 non-conformity.
7. **Impact Analysis** – An analysis of the likely impact on the operations/ activity of the organization
8. **Corrective Action** – The action taken to correct the non-conformity

**Table 2: For follow on/ follow up system audit**

<b>Preliminary Audit Date</b>	<b>Preliminary Audit Period</b>	<b>Preliminary Observation Number</b>	<b>Preliminary Status</b>	<b>Preliminary Corrective Action as proposed by Auditor</b>	<b>Current Finding</b>	<b>Current Status</b>	<b>Revised Corrective Action, if any</b>	<b>Deadline for the Revised Corrective Action</b>	<b>Reason for delay in implementation/compliance</b>

**Description of relevant Table heads**

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

\*\*\*\*\*

### Annexure X

1. In order to ensure compliance with the guidelines for Business Continuity Plan (BCP) and Disaster Recovery (DR), prescribed at Para 9.1 of this Chapter of Master Circular for Stock Exchanges and Clearing Corporations, LPCC is permitted to have arrangements with any of the existing Clearing Corporations who are in compliance with the existing regulatory BCP/DR requirements. However, for any issues / disputes arising on account of such arrangement, the LPCC shall be liable. Hence, the LPCC shall incorporate necessary provision into its agreement with the service providers for its BCP/DR arrangement with them.
2. Similarly, in order to ensure compliance with the requirements relating to the prescribed Cyber Security and Cyber Resilience framework at Para 10.1 and 10.6 of this Chapter of Master Circular for Stock Exchanges and Clearing Corporations, LPCC is permitted to have outsourcing arrangements for cyber security with any of the existing Clearing Corporations for the purposes of Cyber Security. For any issues / disputes arising on account of such arrangement, LPCC would be liable.

## ANNEXURE XI

### Standard Operating Procedure (SOP) for handling of technical glitches

#### Definition of "Technical Glitch"

1. Technical glitch shall mean any malfunction in the systems of an MII. Malfunction in the systems of the MII shall include malfunction in its (a) hardware, or; (b) software, or; (c) any products/ services provided by the MII, whether on account of inadequate infrastructure/ systems or otherwise, which may lead to either stoppage or variance in the normal functions/ operations of systems of the MII.

#### Reporting Requirements

2. The following reporting structure for technical glitches shall be adopted by the MIIs:

Sl. No.	Disruption	Reporting
1.	No business disruption	<ul style="list-style-type: none"> <li>• Standing Committee on Technology (SCOT) of MII</li> <li>• Governing Board of MII</li> </ul>
2.	Business disruption	<ul style="list-style-type: none"> <li>• SCOT of MII</li> <li>• Governing Board of MII</li> <li>• SEBI</li> </ul>

Business disruption shall mean either stoppage or variance in the normal functions/operations of systems of the MII thereby impacting normal/regular service delivery of the MII.

- 2.1. With regard to incidents resulting in business disruption, the following shall be submitted by the MIIs to SEBI:
  - (i) Information of technical glitch on immediate basis but not later than 2 hours from the time of occurrence of the glitch; provided that glitches of the nature of a disaster- as defined above in Clause 9.1.2.3 - shall be reported immediately upon declaration of disaster.
  - (ii) Preliminary report within 24 hours of the occurrence of the glitch.
  - (iii) Comprehensive Root Cause Analysis (RCA) report and corrective action taken to address the technical glitch within 21 days of the incident. Such report shall be submitted to SEBI, after placing the same before the Standing Committee on Technology and the Governing Board of the MII and confirming compliance with their observations.
  - (iv) RCA submitted by the MIIs should inter-alia include exact cause of the technical glitch (including root cause from vendor(s), if applicable), exact duration of the technical glitch, chronology of events, list of business processes/systems and time for which they were impacted, recommendations of SCOT / Governing Board of MII, details of

corrective/ preventive measures taken (or to be taken) by MII along with timelines and any other aspect relevant to the technical glitch. As part of the RCA, MIIs are required to demonstrate compliance with various requirements of this SOP. The RCA shall include details regarding time of incident, time when operations were restored and in the event of a disaster, time when disaster was declared.

- 2.2. All communication and information with regard to technical glitch shall be shared by the MII with SEBI through a dedicated e-mail id viz. [techglitch@sebi.gov.in](mailto:techglitch@sebi.gov.in)
- 2.3. SEBI on identification of the Technical Glitch resulting into Financial Disincentive to the MIIs, or upon receipt of the information of any such instance shall provide an opportunity to the concerned MIIs to make their submissions in respect of the facts of the case.
- 2.4. MIIs shall carry out internal examination pertaining to occurrence of technical glitches to ascertain individual accountability and take appropriate action including suitable recording and reckoning in the performance appraisal of those individuals. SEBI would retain the right to initiate enforcement action against the individuals at the MII, if there is sufficient ground to do so.

#### **Placing before Technical Advisory Committee (TAC)**

3. With regard to the incidents wherein business is disrupted, the RCA and corrective action taken, as submitted by the MII, shall be placed before TAC of SEBI. TAC/ SEBI, if it so desires, may seek additional information/ clarification from the MII regarding the technical glitch.
4. In case TAC finds the actions taken by the MII as inadequate, then, based on the recommendations of TAC, the MII shall be required to address the technical glitch by taking appropriate corrective actions, within the timeline specified by TAC/SEBI. While deciding such timeline, criticality of the malfunction and/or the services/ applications affected by the same shall also be taken into consideration.

## ANNEXURE XII

### “Financial Disincentive” structure with regard to handling of technical glitches

#### Failure to timely submit RCA

1. In case of delay in submission or submission of incomplete/ inadequate RCA by an MII, a “financial disincentive” of Rs.1,00,000 per working day shall be paid by the MII for each working day of delay from the timeline specified at Para 2.1(iii) of Annexure XI above or any revised timeline specified by TAC/SEBI for submission of exact RCA.

#### Failure to timely address technical glitch

2. In order to ensure that MIIs address technical glitch within the timeline specified by TAC/SEBI, the following progressive slab-wise “financial disincentive” shall be paid from the expiry of the timeline specified by TAC/ SEBI:

S No.	No. of working days during which failure continues (i.e. after expiry of the timeline specified by TAC/ SEBI)	Financial disincentive to be paid by the MII (Rs.)
i.	First 15 working days	2 lakh per working day
ii.	Subsequent 15 working days	3 lakh per working day in addition to S No. (i) above
iii.	Beyond 30 working days	25 lakh in addition to S No (i) and (ii) above

#### Failure to declare disaster within stipulated timelines

3. It has been mandated that, in the event of disruption of any one or more of the ‘Critical Systems’, the MII shall, within 30 minutes of the incident, declare that incident as ‘Disaster’. In case of delay in declaration of disaster beyond the timeline specified by SEBI, the following “financial disincentive” shall be paid:

S No.	Delay in declaration of disaster beyond abovementioned timeline specified by SEBI	Financial disincentive Equivalent (Rs.)
i.	Financial disincentive on MII	10% of average of standalone net profit for previous two financial years or Rs. 2 cr., whichever is higher.

#### Failure to restore operations within Recovery Time Objective (RTO)

4. In the event of a disaster, if an MII fails to restore its operations within the RTO prescribed by SEBI, i.e. to restore operations of ‘Critical Systems’ including from Disaster Recovery Site within 45 minutes of declaration of Disaster, the following “financial disincentive” shall be paid:

<b>S No.</b>	<b>Failure to restore operations within the RTO prescribed by SEBI</b>	<b>Financial disincentive Equivalent (Rs.)</b>
i.	Financial disincentive on MII	10% of average of standalone net profit for previous two financial years or Rs. 2 cr., whichever is higher.

“Financial disincentive” under Clause 3 and Clause 4 above, in relation to the same disaster, shall be paid only once either under Clause 3 or Clause 4.

5. Further, if an MII fails to restore operations of Critical Systems including from Disaster Recovery Site within three hours from the occurrence of the disaster, the following additional “financial disincentive” (over and above S No 3 or 4 above) shall be paid:

<b>S No.</b>	<b>Failure to Restore operations of Critical systems beyond abovementioned timeline</b>	<b>Financial disincentive Equivalent (Rs.)</b>
i.	Financial disincentive on MII	10% of average of standalone net profit for previous two financial years or Rs. 2 cr., whichever is higher.

**Failure to restore normalcy in cases of business disruption, not being in the nature of a Disaster**

6. In the event of any business disruption, which is not required to be declared as “Disaster”, if an MII fails to restore normalcy of operations within 75 minutes of the incident, the following slab wise “financial disincentive” shall be paid by the MII:

<b>S No.</b>	<b>Failure to Restore normalcy within</b>	<b>Financial disincentive (Rs.)</b>
i.	75 minutes to 3 hours of the incident	Rs. 50 lacs
ii.	Beyond 3 hours of the incident	Rs.1 crore

7. The amount of “financial disincentive” paid as per the above structure shall be credited by MII to the following funds maintained by it:

<b>S No.</b>	<b>Financial Disincentive on MIIs</b>	<b>Credited to Funds</b>
i.	Stock Exchange	Investor Protection Fund (IPF)
ii.	Clearing Corporation	Core Settlement Guarantee Fund (Core SGF)
iii.	Depositories	Investor Protection Fund (IPF)

8. Further, the MII shall submit a compliance report within 90 days of occurrence of disaster/ business disruption to SEBI providing details of payment of “financial disincentives” including computation of “financial disincentives” as per the SOP and the date when the amount was credited to the aforementioned funds.
9. MIIs shall disclose on their websites (and in their respective annual reports), the details of financial disincentive paid by them on account of technical glitches. Further, listed MIIs shall make appropriate disclosures required in terms of SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 regarding any financial disincentive imposed by SEBI on account of technical glitch.
10. The financial disincentives automatically triggered under predefined circumstances as stated in clauses 1, 2, 3, 4, 5, 6 above shall be paid by the MIIs. However, these financial disincentives shall be without prejudice to any action as may be initiated by SEBI.

\*\*\*\*\*

**Annexure XIII**

1. Level of support definitions for outsourcing/in-house are as follows:

1.1. Security Analyst Level 1 (L1): This function may be mostly outsourced

- (a) Monitoring SIEM Solution console for identifying the security events generated by the log sources integrated with SIEM tools.
- (b) Identification of security events that are false +ve before qualifying event as an incident.
- (c) Identify the exceptions which are identified as an event (e.g. VA scanning performed by SEBI appointed 3rd party which may be identified as port scanning attack).
- (d) Perform first level event analysis before qualifying the incidents.
- (e) Qualifying the event as an incident using Knowledgebase.
- (f) Escalating exceptions & Events to L2 level.
- (g) Log Incident tickets in service management tool and assign it to the respective team.
- (h) Follow-up for the closure of the incident tickets generated.

1.2. Security Analyst Level 2 (L2): Combination of Outsource / In-House

- (a) Exception Analysis.
- (b) Analysis of extended events.
- (c) Confirmation of False +ve & update Knowledge Base.
- (d) Qualify Incident & provide mitigation suggestions.
- (e) Escalate incident to next level.
- (f) Update /configuration correlation rules after approval.

1.3. Security Analyst Level 3 (L3): Combination of Outsource / In-House

- (a) Analysis of escalated Incidents.
- (b) Define correlation rules.
- (c) Analysis of impact on SIEM over all correlation rules and operations for the correlation rules suggested by Level 2 Analyst.
- (d) Approve correlation rules after the impact analysis.
- (e) Perform impact analysis before deployment of correlation rules.
- (f) Perform impact analysis for update and upgrade of SIEM & Advance security solutions components.
- (g) Define Mitigation suggestions for newly identified incidents.

(h) Approve the reports before sharing with others.

1.4. SOC Manager (L4) : In-house

- (a) Lead and manage Security Operations Centre.
- (b) Provide strategic directions to SOC team and organization for security posture improvements.
- (c) To identify key contacts for incident escalation and change management activities.
- (d) Ensure compliance to SLA.
- (e) Ensure process adherence and process improvisation to achieve operational objectives.
- (f) Revise and develop processes to strengthen the current Security Operations.
- (g) Responsible for team and vendor management.
- (h) Responsible for overall use of resources and initiation of corrective action where required for Security Operations Center.
- (i) Escalate to the other IT Infra. Management teams or application maintenance teams, as necessary.
- (j) Overall responsibility for delivery of in scope activities as a part of this engagement.
- (k) Point of contact for problem escalation and reporting.

1.5. Security Subject Matter Expert for Security technologies: In-house with reliance on external expertise

- (a) Subject Matter Expert (SME) for SIEM and Advance security solutions.
- (b) Assist you with troubleshooting steps to be performed by you in order to re-establish connectivity between the SIEM System and SEBI's locations.
- (c) Provide software-level management for the SIEM System components;
- (d) Verify data collection and log continuity;
- (e) Manage user access including user and group permissions updates;
- (f) Review application performance, capacity, and availability make recommendations as appropriate;
- (g) Review SIEM System disk space usage;
- (h) Verify time synchronization among SIEM System components;
- (i) Perform archival management and retrieval per change

management process;

- (j) Provide problem determination / problem source identification for the SIEM System, consisting of creating tickets & tracking progress of Open tickets
- (k) Managing tickets to resolution / closure, in accordance with the processes as defined in the Integrated and Transition vendor announcements & manage SIEM System update alerts;
- (l) Install application patches and software updates in order to improve performance, or enable additional functionality

### **Illustrative Training Requirements**

#### **Security Analyst Level 1 (L1):**

- 1) SEC401: Security Essentials Bootcamp Style  
<https://www.sans.org/event/cyber-defence-canberra-2018/course/security-essentials-bootcamp-style>
- 2) SEC301: Introduction to Cyber Security  
<https://www.sans.org/course/introduction-cyber-security>

#### **Security Analyst Level 2 (L2):**

- 1) SEC542: Web App Penetration Testing and Ethical Hacking  
<https://www.sans.org/event/cyber-defence-canberra-2018/course/web-app-penetration-testing-ethical-hacking>
- 2) SEC566: Implementing and Auditing the Critical Security Controls - In-Depth  
<https://www.sans.org/private-training/course/implementing-auditing-critical-security-controls>
- 3) SEC575: Mobile Device Security and Ethical Hacking  
<https://www.sans.org/private-training/course/mobile-device-security-ethical-hacking>

#### **Security Analyst Level 3 (L3):**

- 1) SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling  
<https://www.sans.org/event/cyber-defence-canberra-2018/course/hacker-techniques-exploits-incident-handling>
- 2) FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting  
<https://www.sans.org/event/digital-forensics-summit-2018/course/advanced-incident-response-threat-hunting-training>
- 3) SEC501: Advanced Security Essentials - Enterprise Defender

<https://www.sans.org/private-training/course/advanced-security-essentials-enterprise-defender>

- 4) MGT414: SANS Training Program for CISSP® Certification  
<https://www.sans.org/course/sans-plus-s-training-program-cissp-certification-exam>

**SOC Manager (L4):**

- 1) Cyber Security Specialist  
<http://www.leaderquestonline.com/it-career-training/cybersecurity-specialist/>
- 2) Managing Security Operations: Detection, Response, and Intelligence  
<https://www.sans.org/event/rocky-mountain-2018/course/managing-security-operations-detection-response-and-intelligence>
- 3) SIEM with Tactical Analytics  
<https://www.sans.org/private-training/course/siem-with-tactical-analytics>
- 4) SEC511: Continuous Monitoring and Security Operations  
<https://www.sans.org/course/continuous-monitoring-security-operations>
- 5) SEC599: Defeating Advanced Adversaries - Implementing Kill Chain Defenses  
<https://www.sans.org/course/defeating-advanced-adversaries-kill-chain-defenses>

#### Annexure XIV - Systems deemed to be based on AI and ML technology

Applications and Systems belonging but not limited to following categories or a combination of these:

1. Natural Language Processing (“NLP”), sentiment analysis or text mining systems that gather intelligence from unstructured data. – In this case, Voice to text, text to intelligence systems in any natural language will be considered in scope. Eg: robo chat bots, big data intelligence gathering systems.
2. Neural Networks or a modified form of it. –In this case, any systems that uses a number of nodes (physical or software simulated nodes) mimicking natural neural networks of any scale, so as to carry out learning from previous firing of the nodes will be considered in scope. Eg: Recurrent Neural Networks and Deep Learning Neural Networks
3. Machine learning through supervised, unsupervised learning or a combination of both. – In this case, any application or systems that carry out knowledge representation to form a knowledge base of domain, by learning and creating its outputs with real world input data and deciding future outputs based upon the knowledge base. Eg: System based on Decision tree, random forest, K mean, Markov decision process, Gradient boosting Algorithms.
4. A system that uses statistical heuristics method instead of procedural algorithms or the system / application applies clustering or categorization algorithms to categorize data without a predefined set of categories.
5. A system that uses a feedback mechanism to improve its parameters and bases its subsequent execution steps on these parameters.
6. A system that does knowledge representation and maintains a knowledge base.

**Annexure XV - Form to report on AI and ML technologies - to be submitted quarterly**

S/N	Head	Value
1	Entity SEBI registration number	
2	Registered entity category	
3	Entity name	
4	Entity PAN no.	
5	Application / System name	
6	Date used from	
7	Type of area where AI or ML is used (order execution / Surveillance / compliance / others). In case of others, please specify.	
8	What is the name of the Tool / Technology that is categorized as AI and ML system / Application and submissions are declared vide this response	<free text field>
9	How was the AI or ML project implemented	<Internally / through solution provider / Jointly with a solution provider or third party>
10	Are the key controls and control points in your AI or ML application or systems in accordance with circular(s) of SEBI that mandate/s cyber security control requirements	<free text field>
11	Is the AI / ML system included in the system audit	<Yes / No>
12	Describe the application / system and how it uses AI / ML	<free text field>
13	What safeguards are in place to prevent abnormal behavior of the AI or ML application / System	<free text field>