Member Technology Related Compliance

Table of Contents

CHAPTER 1 3
System Audit of Members of the Exchange 3
Auditor Selection Norms 5
Penalty/Disciplinary Actions: 6
CHAPTER 2 9
Cyber Security and Cyber Resilience Audit.....9
Auditor Selection Norms 10
Penalty/Disciplinary Actions 12
CHAPTER 3 15
Cyber Incident Reporting and information sharing 15
CHAPTER 4 16
Vulnerability Assessment and Penetration Testing (VAPT).....16
Penalty/Disciplinary Actions 16
CHAPTER 5 21
Framework to address the 'Technical Glitches' in Member's Electronic Trading Systems 21
ANNEXURE A.....21
Penalty / Disciplinary Action 26
CHAPTER 6 29
Artificial Intelligence (AI) and Machine Learning (ML) applications.....29
Scope definition 29
Regulatory requirements.....29
CHAPTER 7 32
Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs) 32
CHAPTER 8 33
Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions 33
CHAPTER 9 34
Advisory for SEBI Regulated Entities (REs) regarding Cybersecurity best practices..34
Glossary 115

CHAPTER 1
System Audit of Members of the Exchange

In terms of provisions of the Rules, Bye-Laws and Business Rules of the Exchange and in continuation to SEBI circular no. CIR/MRD/DMS/34/2013 dated November 6, 2013, Exchange circular no. MCX/CTCL/423/2017 dated November 15, 2017 and Exchange circular no. MCX/CTCL/167/2021 dated March 19, 2021 Members are required to submit system audit report as per the norms specified therein.

As per the provision of Master Circular, Trading Members are required to undertake system audit of their software for the period through System Auditor as per Auditor Selection Norms and submit the System Audit Report (SAR) to the Exchange within the timeline as mentioned in the table below:

Periodicity of System	**Criteria**	**Type of Broker**	**Due Date for Submission of Reports**	
			System Audit Report	**Action Taken Report, if applicable**
Half Yearly (October 2023 to March 2024)	Members using ATF Facility	Type of Broker - III	June 30, 2024	September 30, 2024
Annual / Yearly (April 2023 to March 2024)	1. Members using CTCL Facility with presence in > 10 locations or have > 50 terminals 2. Trading Members who are also depository participants or are involved in offering any other financial services	Type of Broker-II	June 30, 2024	September 30, 2024
Once in 2 years (April 2022 to March 2024)	Members using CTCL Facility with presence in < 10 locations or have < 50 terminals	Type of Broker-II	June 30, 2024	September 30, 2024

Members are required to submit the System Audit Report online through Member Portal - https://member.mcxindia.com. Terms of Reference (ToR) – Type II & Type III are incorporated in the online Member portal and **'System Audit Report – Help File'** is available on the portal and on shared path https://sftp.mcxindia.com/Common/Online portal help files folder.

The online SAR portal will be available only to the applicable Members for audit report submission as per the schedule specified below:

Periodicity of System Audit	Report Submission Period
Half Yearly (October 2023 – March 2024)	Till June 30, 2024
Annual (April 2023 – March 2024)	Till June 30, 2024
Once in 2 years (April 2022 – March 2024)	Till June 30, 2024

All Trading members are requested to take note that, for each non-compliance reported by the auditor, trading members are required to submit corrective action taken report as per above mentioned timelines. On review of details of corrective action submitted by trading member, the auditor shall submit the status of compliance as Compliant or Non-Compliant.

Submission of System Audit Report with Management comments shall be considered complete only after Member submits the report to the Exchange and receives an acknowledgment email. Saved reports/reports submitted by auditor will not be considered as final submission. Further, auditor has to provide compliance status for each TOR item i.e., Compliant/Non-Compliant and Not Applicable and in case of any TOR item which is not applicable, auditor is required to provide justification for the non-applicability of said TOR.

Members are requested to refer to the below mentioned documents while submitting the system audit report.

- Details of Auditor – **Annexure 1**
- Terms of Reference (ToR for type II and Type III) – **Annexure 2**

Auditor Selection Norms:

1. The Auditor should have experience of IT audit/governance frameworks and processes conforming to industry leading practices like COBIT 5/ISO 27001.

2. The Auditor shall have a minimum of 3 years of experience in IT audit of securities market participants e.g., Stock Exchanges, Clearing Corporations, Depositories, Trading Member, 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.

3. The Auditor/Auditor firm can perform a maximum of 3 successive audits of the Trading Member. Follow-on audit conducted by the auditor shall not be considered in the successive audits. However, such an auditor shall be eligible for re-appointment after a cooling-off period of one year.

4. Resources employed for the purpose of system audit should possess at least one of the following certifications:

   - CISA (Certified Information System Auditors) from ISACA
   - DISA (Post Qualification Certification in Information Systems Audit) from Institute of Chartered Accountants of India (ICAI)
   - CISM (Certified Information Security Manager) from ISACA
   - CISSP (Certified Information Systems Security Professional) from International
   - Information Systems Security Certification Consortium, commonly known as (ISC)2.

5. The Auditor, as being appointed by Trading Member must not have any conflict of interest in conducting fair, objective, and independent audit. Further, the directors / partners of Audit firm shall not be related to any Directors/Promoters/Proprietor of the said Trading Members either directly or indirectly.

6. Auditor should not have been engaged over the last three years in any consulting engagement with any departments / units of the Trading Member.

7. 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.

The trading members and auditors are required to retain records of physical visits conducted during audits like name, qualification & date of visit/s of auditor, along with audit artifacts, proofs of concept (POCs), and evidence related to terms of reference (TOR) points for a minimum duration of three years.

Penalty/Disciplinary Actions:

As per the circular no. MCX/TECH/856/2023 dated December 11, 2023 on "*Revised Penalties/disciplinary action(s)/charges for System Audit Report and Cyber Security & Cyber Resilience Audit Report related submissions*" The revised penalty/disciplinary action(s) with respect to any delay or non-submission of Preliminary Audit Report, Action Taken Report (ATR) and/or Follow-on audit report are stipulated in Table- A below:

Annexure – 1 Penalty/Disciplinary action for Delayed / Non-submission of Preliminary audit / ATR / Follow-on audit Report

Details of Violation	**Period of violation**	**Penalty/disciplinary actions**	**Penalty/disciplinary action in case of repeated violation**
Delay / Non submission of Preliminary audit/ATR / Follow on audit report as recommended by the auditor in case of System Audit report / Cyber Security and Cyber Resilience Audit report.	From 1st day to 7th day:	Charges Rs. 1,500/- per day for Non QSB & Rs. 3,000/- per day for QSB from the due date till first 7 calendar days or submission of report, whichever is earlier.	In case of a repeat instance by the Member, levy of applicable monetary penalty along with an escalation of 50%.
	From 8th day to 21st day:	Charges of Rs. 2,500/- per day for Non QSB & Rs. 5,000/- per day for QSB from 8th calendar day after the due date to 21st calendar day or submission of report, whichever is earlier.	Levy of applicable monetary penalty along with an escalation of 50%.
	From 22nd day onwards:	In case of non-submission of report till 21st calendar days, new client registration shall be prohibited and notice of 7 calendar days for disablement of trading facility till submission of report, shall be issued. The disablement notice issued to the member will be shared with all the Exchanges for information.	
	After 28th day:	In case of non-submission of report by 28th calendar day, Member shall be disabled in all segments till submission of report.	

Further, members are required to submit closure status of all the non-compliances reported in System Audit and Cyber Security and Cyber Resilience Audit by submitting Action Taken Report (ATR) within the prescribed timelines. To ensure strict adherence for closure of non-compliances within the prescribed timelines, the following penalty as provided in Table-B shall be applicable for non-closure of observations reported in ATR submissions.

Annexure – 2 Penalty/Disciplinary action for Non- closure of observations reported in System Audit Report & Cyber Security and Cyber Resilience Audit Report

Risk rating reported by auditor	**Applicable penalties for each High/Medium/Low risk non-closure of non-Compliances, which have not been closed in ATR (i.e., within prescribed timelines of submission of due date of preliminary audit report)**			
	Non QSB Members		**QSB Members**	
	System Audit Report	**Cyber Audit Report**	**System Audit Report**	**Cyber Audit Report**
High Risk	₹ 15,000	₹ 50,000	₹ 30,000	₹ 100,000
Medium Risk	₹ 7,500	₹ 25,000	₹ 15,000	₹ 50,000
Low Risk	₹ 2,500	₹ 5,000	₹ 5,000	₹ 10,000

- In case observations are not closed by members within three weeks from the due date for submission of Action Taken Report (ATR), new client registration to be prohibited and notice of 7 days for disablement of trading facility till closure of observation(s).
- The disablement notice issued to the member shall be shared with all the Exchanges for information. In case of non-closure of observation(s) within four weeks from the due date of submission of ATR, Member shall be disabled in all segments until closure of observations(s).

The provisions of this circular shall be applicable from the System Audit and Cyber Security and Cyber Resilience Audit Report submissions for half year ended September 2023 and onwards.

Circulars for reference

Issued by	Circular Dated	Circular No	Particulars
SEBI	November 6, 2013	CIR/MRD/DMS/34/2013	Annual System Audit of Stock Brokers / Trading Members
MCX	November 15, 2017	MCX/CTCL/423/2017	Master Circular – Computer to Computer Link (CTCL)
MCX	March 19, 2021	MCX/CTCL/167/2021	System Audit of Trading Member
MCX	March 31, 2023	MCX/CTCL/213/2023	Uniform Terms of Reference for System Audit
MCX	May 18, 2023	MCX/CTCL/324/2023	System Audit of Trading Member
MCX	December 11, 2023	MCX/TECH/856/2023	Revised Penalties/disciplinary action(s)/charges for System Audit Report and Cyber Security & Cyber Resilience Audit Report related submissions

CHAPTER 2
Cyber Security and Cyber Resilience Audit

In terms of provisions of the Rules, Bye-Laws and Business Rules of the Exchange and in continuation to SEBI circular no. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018, SEBI/HO/MIRSD/DOP/CIR/P/2019/109 dated October 15, 2019, SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022, SEBI/HO/MIRSD/TPD/P/CIR/2022/93 dated June 30, 20222, Exchange circular no. MCX/CTCL/423/2017 dated November 15, 2017 and MCX/TECH/168/2021 dated March 19, 2021, Members are required to submit Cyber Security & Cyber Resilience Audit report as per the norms specified therein.

As per the provision of Exchange Circular, Trading Members are required to undertake Cyber Security & Cyber Resilience Audit for the period specified below through System Auditor appointed as per Auditor Selection Norms and submit the Cyber Security & Cyber Resilience Audit Report (CSCR) to the Exchange within the timeline as mentioned in the table below:

Periodicity of Audit	**Criteria**	**Type of Broker**	**Due Date for Submission of Reports**	
			Audit Report	**Action Taken Report, if applicable**
Annual / Yearly (April 2023 – March 2024)	Members trading through Exchange provided Trader Work Station (TWS)	Type of Broker-I	June 30, 2024	September 30, 2024
Annual / Yearly (April 2023 – March 2024)	Members using CTCL Facility	Type of Broker-II	June 30, 2024	September 30, 2024
Half Yearly (October 2023 – March 2024)	Members using ATF facility	Type of Broker-III	June 30, 2024	September 30, 2024

Members are required to submit the Cyber Security & Cyber Resilience Audit Report online through Member Portal – https://member.mcxindia.com. Terms of Reference (ToR)

– Type I, II & III are incorporated in the online Member portal and **'Cyber Security & Resilience Audit Reporting – help file'** is available on the CSCR online portal and on https://sftp.mcxindia.com/Common/Online portal help file folder.

All Trading members are requested to take note that, for each non-compliance reported by the auditor, trading members are required to submit corrective action taken report as per above mentioned timelines. On review of details of corrective action submitted by trading member, the auditor shall submit the status of compliance as Compliant or Non-Compliant.

Submission of Cyber Security and Cyber Resilience Audit Report shall be considered complete only after trading member submits the report to the Exchange after providing management comments. Further, auditor must provide compliance status for each TOR item as Compliant/Non-Compliant/Not Applicable and in case of any TOR item which is not applicable, auditor is required to provide justification for non-applicability of said TOR.

The online Cyber Security & Cyber Resilience Audit portal will be available only to the applicable Members for audit report submission as per the above mentioned due dates.

Members are requested to refer to the following documents while submitting the Cyber audit report.

- Details of Auditor – **Annexure 3**
- Terms of Reference – **Annexure 4**

Member Categorization

Sr. No.	Type of Members and Periodicity	Audit Period
1	**Type I** Member using trading software provided by the Exchange (TWS) and software provided by Application Service Provider (ASP)	April-March (12 Months)
2	**Type II – Annual** Members using CTCL Facility	April-March (12 Months)
3	**Type III – Half Yearly** All Members using ATF Facility	April-September
		October-March

Auditor Selection Norms

1. The Audit shall be conducted by CERT-In empanelled organization/ entity.

2. The Auditor/Auditor firm can perform minimum of 3 successive audits of the Trading Members. However, such an auditor shall be eligible for reappointment after a cooling – off period of one year.

3. The Auditor, as being appointed by Trading Member must not have any conflict of interest in conducting fair, objective, and independent audit. Further, the directors / partners of Audit firm shall not be related to any Directors/Promoters/Proprietor of the said Trading Members either directly or indirectly.

4. Auditor should not have been engaged over the last three years in any consulting engagement with any departments / units of the Trading Member.

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.

6. The trading members and auditors are required to retain records of physical visits conducted during audits like name, qualification & date of visit/s of auditor, along with audit artifacts, proofs of concept (POCs), and evidence related to terms of reference (TOR) points for a minimum duration of three years.

Members are requested to note the list of Cyber Auditors is available in the above mentioned portal. Kindly submit attached Annexure 3 (E-Mail to reporting@mcxindia.com) to update the Auditor details which are not reflecting in online Cyber Security & Cyber Resilience Audit portal of Exchange

Penalty/Disciplinary Actions

As per the MCX circular no. MCX/TECH/856/2023 dated December 11, 2023 on "*Revised Penalties/disciplinary action(s)/charges for System Audit Report and Cyber Security & Cyber Resilience Audit Report related submissions*", the revised penalty/disciplinary action(s) with respect to any delay or non-submission of Preliminary Audit Report, Action Taken Report (ATR) and/or Follow-on audit report are stipulated in Table- A below:

Annexure – 1 Penalty/Disciplinary action for Delayed / Non-submission of Preliminary audit / ATR / Follow-on audit Report

Details of Violation	**Period of violation**	**Penalty/disciplinary actions**	**Penalty/disciplinary action in case of repeated violation**
Delay/ Non submission of Preliminary audit/ATR / Follow on audit report as recommended by the auditor in case of System audit report /Cyber Security and Cyber Resilience Audit report.	From 1st day to 7th day	Charges Rs. 1,500/- per day for Non QSB & Rs. 3,000/- per day for QSB from the due date till first 7 calendar days or submission of report, whichever is earlier.	In case of a repeat instance by the Member, levy of applicable monetary penalty along with an escalation of 50%.
	From 8th day to 21st day	Charges of Rs. 2,500/- per day for Non QSB & Rs. 5,000/- per day for QSB from 8th calendar day after the due date to 21st calendar day or submission of report, whichever is earlier.	Levy of applicable monetary penalty along with an escalation of 50%.
	From 22nd day onwards	In case of non-submission of report till 21st calendar days, new client registration shall be prohibited and notice of 7 calendar days for disablement of trading facility till submission of report, shall be issued. The disablement notice issued to the member will be shared with all the Exchanges for information.	
	After 28th day	In case of non-submission of report by 28th calendar day, Member shall be disabled in all segments till submission of report.	

Further, members are required to submit closure status of all the non-compliances reported in System Audit and Cyber Security and Cyber Resilience Audit by submitting Action Taken Report (ATR) within the prescribed timelines. To ensure strict adherence for closure of non-compliances within the prescribed timelines, the following penalty as provided in Table-B shall be applicable for non-closure of observations reported in ATR submissions.

Annexure – 2 Penalty/Disciplinary action for Non- closure of observations reported in System Audit Report & Cyber Security and Cyber Resilience Audit Report

Risk rating reported by auditor	**Applicable penalties for each High/Medium/Low risk non-closure of non-Compliances, which have not been closed in ATR (i.e., within prescribed timelines of submission of due date of preliminary audit report)**			
	Non QSB Members		**QSB Members**	
	System Audit Report	**Cyber Audit Report**	**System Audit Report**	**Cyber Audit Report**
High Risk	₹ 15,000	₹ 50,000	₹ 30,000	₹ 100,000
Medium Risk	₹ 7,500	₹ 25,000	₹ 15,000	₹ 50,000
Low Risk	₹ 2,500	₹ 5,000	₹ 5,000	₹ 10,000

- In case observations are not closed by members within three weeks from the due date for submission of Action Taken Report (ATR), new client registration to be prohibited and notice of 7 days for disablement of trading facility till closure of observation(s).
- The disablement notice issued to the member shall be shared with all the Exchanges for information. In case of non-closure of observation(s) within four weeks from the due date of submission of ATR, Member shall be disabled in all segments until closure of observations(s).

The provisions of this circular shall be applicable from the System Audit and Cyber Security and Cyber Resilience Audit Report submissions for half year ended September 2023 and onwards.

Circulars for reference

Issued by	Circular Dated	Circular No	Particulars
SEBI	December 03, 2018	SEBI/HO/MIRSD/CIR/PB/ 2018/147	Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants
SEBI	October 15, 2019	SEBI/HO/MIRSD/DOP/ CIR/P/2019/109	Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants - Clarifications
MCX	November 15, 2017	MCX/CTCL/423/2017	Master Circular – Computer to Computer Link (CTCL)
MCX	January 31, 2019	MCX/TECH/058/2019	Cyber Security & Cyber Resilience Audit of Member
MCX	October 16, 2019	MCX/TECH/587/2019	Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants - Clarifications
MCX	March 31, 2023	MCX/TECH/214/2023	Uniform Terms of Reference for Cyber Security & Cyber Resilience Audit
MCX	May 18, 2023	MCX/TECH/325/2023	Cyber Security & Cyber Resilience Audit
MCX	December 11, 2023	MCX/TECH/856/2023	Revised Penalties/disciplinary action(s)/charges for System Audit Report and Cyber Security & Cyber Resilience Audit Report related submissions

CHAPTER 3
Cyber Incident Reporting and information sharing

All Cyber-attacks, threats, cyber-incidents and breaches experienced by Member shall be reported to Stock Exchanges / SEBI.

The incident shall also be reported to Indian Computer Emergency Response team (CERT-In) in accordance with the guidelines / directions issued by CERT-In from time to time. Additionally, the Member, whose systems have been identified as "Protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC.

The quarterly reports containing information on cyber-attacks, threats, cyber-incidents and breaches experienced by Member and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities, threats that may be useful for other Member / Depository Participants / Exchanges /Depositories and SEBI shall be submitted to Stock Exchanges / Depositories within 15 days from the quarter ended June, September, December and March of every year on exchange portal, as per specific format (attached as **Annexure 5**) The above information shall be shared to SEBI through the dedicated e-mail id: **sbdp-cyberincidents@sebi.gov.in**.

Also, all the Trading Members of the Exchange are required to report Cyber Incident(s) whether occurred /non-occurred for the quarter ending **through portal https://sftp.mcxindia.com/Common**.

The help file for online submission is available on SFTP common path: https://sftp.mcxindia.com/Common.

Non-compliant members shall render themselves liable for action as may be deemed fit by the Exchange**.**

Circulars for Reference

Issued by	Circular Dated	Circular No	Particulars
SEBI	December 03, 2018	SEBI/HO/MIRSD/CIR/PB/ 2018/147	Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants
MCX	December 13, 2018	MCX/TECH/524/2018	Cyber Security and Cyber Resilience framework for Members
MCX	January 31, 2019	MCX/TECH/058/2019	Cyber Security & Cyber Resilience Audit of Member
MCX	July 19, 2019	MCX/TECH/375/2019	Information sharing on Cyber Security incident
SEBI	October 15, 2019	SEBI/HO/MIRSD/DOP/CIR/P /2019/109	Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants-Clarifications
MCX	October 16, 2019	MCX/TECH/587/2019	Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants-Clarifications

CHAPTER 4
Vulnerability Assessment and Penetration Testing (VAPT)

Members are required to conduct and complete the VAPT during the period September to November for FY 2023-24 and the final report shall be submitted through member portal to the Stock Exchanges within one month from the date of completion of VAPT after approval from Technology Committee of respective Stockbrokers.

The detailed VAPT report along with summary of report (as per format specified **Annexure – 6)** in as a single document shall be digitally signed by CERT-In empaneled entity to be submitted to Exchange by December 31, 2023 through online Member Portal – https://member.mcxindia.com Help file 'VAPT–help file' is available on the VAPT submission online portal and on https://sftp.mcxindia.com/Common/Online portal help file folder.

For example:

Audit period	Period to conduct VAPT	Submission of report
2023-2024	Sept 2023 to Nov 2023	December 31, 2023

Further, as per para 44 of SEBI Circular No. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 amended vide SEBI Circular No. SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022 requires that any gaps / vulnerabilities detected shall be remedied on immediate basis and compliance of closure of findings identified during VAPT shall be submitted to the Stock Exchanges within 3 months post the submission of final VAPT report. For any open vulnerabilities as reported & submitted in VAPT report, members are required to submit Compliance Report in the format attached as **Annexure – 7** digitally signed by the CERT-In empaneled entity as appointed by the Member.

In view of the above, Stockbrokers/Trading Members/Qualified Stockbrokers are advised as under:

a) Adherence with the reporting timelines for submission of VAPT report and Compliance report/Action Taken Report (ATR) to the Exchange.

b) Ensure that all open gaps / vulnerabilities are closed within prescribed timelines and are accordingly confirmed in the Compliance report.

Penalty/Disciplinary Actions

In order to ensure strict adherence to the regulatory requirements by Members with the prescribed framework applicable for VAPT submission and timely closure of vulnerabilities, following penalty structure has been prescribed and shall come into effect from submissions of FY 2023-24 (Including Half yearly for QSB's) and onwards.

Sr. No.	Particulars
1	Table A – Non-submission of VAPT report and/or compliance report within below specified dates by Members (other than QSB's).
2	Table B – Non-submission of VAPT report and/or compliance report within below specified dates by QSB's Members.
3	Table C – Penalty/Disciplinary actions applicable in case of non-closure of per open vulnerabilities as reported in VAPT report within period of 3 months.

Table A – Non-submission of VAPT report and/or compliance report within below specified dates by Members (other than QSB's):

Details of Violation	Penalty/Disciplinary actions	Penalty/disciplinary action in case of repeated violation
Non-submission of VAPT report **on or before December 31** and/or Compliance report **on or before March 31**.	1.Charges Rs. 1,500/- per day till first 7 calendar days or submission of report, whichever is earlier. 2. Charges of Rs. 2,500/- per day from 8th calendar day to 21st calendar day or submission of report, whichever is earlier. 3.In case of non-submission of report till 21st calendar days, new client registration shall be prohibited and notice of 7 calendar days for disablement of trading facility till submission of report, shall be issued. 4.The disablement notice issued to the member will be shared with all the Exchanges for information. 5.In case of non-submission of report by 28th calendar day, Member shall be disabled in all segments till submission of report.	In case of a repeat instance by the Member, levy of applicable monetary penalty along with an escalation of 50%. In case of non-submission of report till 21st calendar days, new client registration shall be prohibited and notice of 7 calendar days for disablement of trading facility till submission of report, shall be issued. The disablement notice issued to the member will be shared with all the Exchanges for information. In case of nonsubmission of report by 28th calendar day, Member shall be disabled in all segments till submission of report.

Table B – Non-submission of VAPT report and/or compliance report within below specified dates by QSB's Members:

Details of Violation	**Penalty/disciplinary actions**	**Penalty/disciplinary action in case of repeated violation**
Non-submission of VAPT report **on or before June 30th / December 31** and/or Compliance report **on or before September 30th / March 31.**	1.Charges Rs. 3,000/- per day till first 7 calendar days or submission of report, whichever is earlier 2.Charges of Rs. 5,000/- per day from 8th calendar day to 21st calendar day or submission of report, whichever is earlier 3.In case of non-submission of report till 21st calendar days, new client registration shall be prohibited and notice of 7 calendar days for disablement of trading facility till submission of report, shall be issued. 4.The disablement notice issued to the member will be shared with all the Exchanges for information. 5. In case of non-submission of report by 28th calendar day, Member shall be disabled in all segments till submission of report.	In case of a repeat instance by the Member, levy of applicable monetary penalty along with an escalation of 50%. In case of non-submission of report till 21st calendar days, new client registration shall be prohibited and notice of 7 calendar days for disablement of trading facility till submission of report, shall be issued. The disablement notice issued to the member will be shared with all the Exchanges for information. In case of non-submission of report by 28th calendar day, Member shall be disabled in all segments till submission of report

Table C – Penalty/Disciplinary actions applicable in case of non-closure of per open vulnerabilities as reported in VAPT report within period of 3 months as specified hereunder: -

Categories of Risks	**For All Members (other than QSBs)**	**For QSB Members**
	Non closure of open vulnerabilities by March 31	**Non closure of open vulnerabilities by March 31 (for HY September 30) and by September 30 (for HY March 31)**
High/critical Risk	Rs.50,000/-	Rs.1,00,000/-
Medium Risk	Rs.25,000/-	Rs.50,000/-
Low Risk	Rs.10,000/-	Rs.20,000/-
Apart from the monetary penalty mentioned above, if **High/Critical/Medium** vulnerability is not closed by member within 21 days from the due date of submission of compliance report, new client registration shall be prohibited and notice of 7 days for disablement of trading facility shall be issued. If the vulnerability is not closed during this notice period, then member shall be disabled in all segments till closure of the vulnerability. The disablement notice issued to the member will be shared with all the Exchanges for information.		

The penalty/disciplinary action as mentioned above shall come into effect from submissions of FY 2023-24 (Including Half yearly for QSB's) and onwards.

Circulars for reference

Issued by	**Circular Dated**	**Circular No**	**Particulars**
SEBI	June 07, 2022	SEBI/HO/MIRSD/TPD/P/CIR /2022/80	Modification in Cyber Security and Cyber resilience framework for Stock Brokers / Depository Participants
MCX	July 1, 2022	MCX/TECH/395/2022	Modification in Cyber security and Cyber resilience framework for Stock Brokers Depository Participants
MCX	August 24, 2022	MCX/TECH/491/2022	Modification in Cyber Security and Cyber resilience framework for Stock Brokers

MCX	September 21, 2022	MCX/TECH/544/2022	Addendum– Modification in Cyber Security and Cyber resilience framework
MCX	January 05, 2023	MCX/TECH/011/2023	Submission of VAPT Report for FY2022-23
MCX	September 25, 2023	MCX/TECH/641/2023	Submission of VAPT report and/or Action taken report (ATR)/Compliance Report
MCX	December 11, 2023	MCX/TECH/857/2023	Penalties Disciplinary Action(s) charges for Non-submission of VAPT Report and/or Compliance Report and/or non-closure of open vulnerabilities

CHAPTER 5

Framework to address the 'Technical Glitches' in Member's Electronic Trading Systems

Members of the Exchange, through various circulars, and guidelines, issued from time to time, have been required to put in place various measures/controls, to prevent system failures and to ensure the provision of seamless service/facilities to their clients.

In furtherance to the above, in consultation with SEBI and other Exchanges, it has been decided to issue guidelines/ Standard Operating Procedure (SOP) for handling technical glitches at the Members end as well as provide a framework for Capacity Planning, Software Testing, Change management and Business Continuity Planning (BCP)/Disaster Recovery (DR).

The guidelines, as stated in the SEBI circular SEBI/HO/MIRSD/TPD-1/P/CIR/2022/160 dated November 25, 2022, have been enclosed as **'Annexure-A'** and shall be effective from April 1, 2023, and are applicable to all members providing 'Internet and Wireless technology-based trading facility' (IBT/WT) to their clients.

In specific, points 3.viii, 4.vi, 5.i, 5.ii, 5.iii, 6.v, 6.xiii, 6.xiv are only applicable to 'Specified Members', over and above the other points as stated in '**Annexure A**'.

Members registered with the Exchange, having the most Internet and Wireless technology-based (IBT/WT) clients are classified as 'Specified Members' for this purpose.

In adherence to the above and in consultation with other Exchanges, 35 Members have been identified as 'Specified Members'. The list is enclosed herewith as '**Annexure 8**'.

ANNEXURE A

1. Definition

'Technical glitch' shall mean any malfunction in the Member's systems including malfunction in its hardware, software, networks, processes, or any products or services provided by the Member in the electronic form. The malfunction can be on account of inadequate Infrastructure/systems, cyberattacks/incidents, procedural errors, and omissions, or process failures or otherwise, in their own systems or the one outsourced from any third parties, which may lead to either stoppage, slowing down or variance in the normal functions/operations/services of systems of the Member for a contiguous period of **five minutes (5 minutes) or more**.

'Critical Systems' are defined as all IT systems that are related to Trading applications and trading-related services.

2. Reporting Requirements for Technical Glitch Incidents:

All Members shall be required to report to the Exchange any technical glitches as under:

i. All Members shall inform about the technical glitch to the stock exchanges immediately but **not later than 1 hour** from the time of occurrence of the glitch.

ii. Members shall submit a Preliminary Incident Report to the Exchange within **T+1** day of the incident **('T' being the date of the incident)**. The report shall include the date and time of the incident, details of the incident, effect of the incident, and immediate action taken to rectify the problem.

iii. Members shall submit a **Root Cause Analysis (RCA)** Report of the technical glitch to the stock exchange, within **14 days** from the date of the incident. The **RCA report,** for all technical glitch incidents greater than **45 minutes**, shall also be verified by an independent auditor appointed by the Member.

Submission of all the above three reports shall be as per the format provided in **'Annexure 9'** of this circular.

The reporting would be made to a dedicated email address **infotechglitch@nse.co.in**, which is common across the Exchanges.

Financial Disincentives and Penalties with respect to non-compliance has mentioned below

3. Capacity Planning:

i. Increasing number of investors may create an additional burden on the trading system of Members and hence, adequate capacity planning is a prerequisite for Members to provide continuity of services to their clients.

ii. Members shall do capacity planning for the **'Critical Systems'** infrastructure including server capacities, network availability, bandwidth, and the serving capacity of trading applications.

iii. Capacity planning shall be done based on the rate of growth in the number of transactions observed in the past 2 years. This data should be extrapolated to predict the capacity required for the next 3 years.

iv. The capacity planning by Members should be done every year to review the available capacity, peak capacity, and new capacity required to tackle future load on the system. The purpose shall include all '**Critical Systems'** operated in-house or through a Vendor/Application service provider (ASP).

v. Members shall monitor peak load in their **'Critical Systems'** including the trading applications, servers, and network architecture. The Peak load shall be determined based on the highest peak load observed by the Members during a **calendar quarter**. The installed capacity shall be at **least 1.5 times (1.5x)** of the observed peak load.

vi. Members shall deploy adequate monitoring mechanisms within their networks and systems to get timely alerts on the current utilization of capacity going beyond the permissible limit of 70% of its installed capacity.

In case the actual capacity utilization nears 70% of the installed capacity, immediate action shall be taken to avoid a breach of capacity.

vii. Adequate capacity planning and its review should be part of the annual system audit of the Members.

viii. Additionally, to ensure the continuity of services at the primary data center, **'Specified Members'** shall strive to achieve full redundancy in their IT systems that are related to the **'Critical Systems'.**

4. Software testing and change management:

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

ii. Members shall create test-driven environments for all types of software developed by them or their vendors.

iii. Members, during all relevant phases of software development and operations are required to write exhaustive unit test cases and functional test cases covering all positive & negative scenarios, regression testing, security testing, and non-functional testing including performance testing, stress testing, load testing, etc.

iv. Further, Members shall prepare and maintain a traceability matrix between functionalities and test cases for all **'Critical Systems'.**

v. A Minimum number of unit test cases required for every change made in the software should be defined in advance, based on its functionality, and ensure sufficient test coverage around instructions count, branches, and complexities. This would include base cases for the overall platform, plus specific sets of cases for each module under consideration.

vi. In addition to the above, '**Specified Members'** shall perform software testing in **'automated environments'**. The **'automated environments**' shall be mandatorily set up by '**Specified Members'** before **June 30, 2023.**

vii. To ensure system integrity and stability, all changes to the installed system shall be planned, evaluated for risk, tested, approved, and documented. Members shall implement a change management process to avoid any risk arising due to unplanned and unauthorized changes for all its information security assets (hardware, software, network, etc.).

viii. Change management process shall be well documented and approved by the Governing Board of the Member.

ix. The Exchange has provisioned test environments and conducts periodic mocks for Members to test their systems. Members are required to participate in such environments, each time their systems have gone through changes before such changes are made live.

x. Members shall have a documented process/procedure for the timely deployment of patches for mitigating all identified vulnerabilities. The patch management process shall also be approved by the Governing Board of Members.

xi. Members shall periodically update all their assets including Servers, OS, databases, middleware, network devices, firewalls, IDS /IPS desktops, etc. with the latest applicable versions and patches.

xii. Review of Adequate Change Management and Patch Management processes should be part of the system audit of the Members. As a part of the mandated annual System Audit, the System Auditor shall also provide its comments and observations on the said processes, if any.

5. Monitoring mechanism - Applicable to 'Specified Members'

i. Proactively and independently monitoring technical glitches shall be one of the approaches in mitigating the impact of such glitches. In this context, the **'Specified Members'** shall build API-based **Logging and Monitoring Mechanism (LAMA)** to allow stock exchanges to monitor the '**Key Parameters'** of the **'Critical Systems'**. Under this mechanism, **'Specified Members'** shall monitor key systems & functional parameters to ensure that their trading systems function in a smooth manner. Stock exchanges will, through the API gateway, independently monitor these key parameters in real-time to gauge the health of the **'Critical Systems'** of the **'Specified Members'**.

ii. Through the '**LAMA' Gateway**, values of the '**Key Parameters'** listed below should be served by the **'Specified Members'**.

	Key Parameters for 'LAMA'	
Application	**System**	**Network**
1. Log monitoring	1. CPU Utilization	1. Packet Error Counts
2. Requests/ Second	2. Memory Utilization	2. Bandwidth Utilization
3. Avg. response times	3. Disk utilization	3. DNS failures

4. Trading trend analysis related data	4. Database replication and its Health	
5. Trading API failure counts	5. Uptime	
6. Network Latency		

iii. The **'Specified Members'** and the Exchange will preserve the logs of the key parameters for a period of 30 days in the normal course. However, if a technical glitch takes place, the data related to the glitch shall be maintained for a period of 2 years.

'Specified Members' will be notified by the Stock Exchanges, for onward discussion on the implementation and applicability of '**LAMA' and its key parameters**.

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

i. **'Specified Members'** and Members with a minimum client base of **50,000 clients** across all Exchanges, are to mandatorily establish a '**Business Continuity'/ 'Disaster Recovery setup'**.

ii. Members shall put in place a comprehensive BCP-DR policy document outlining standard operating procedures to be followed in the event of any **'Disaster'**.

iii. **'Disaster'** may be defined as scenarios where:
   a. A **45-minute** disruption of any of the **'Critical Systems',** or
   b. Any additional criteria specified by the Governing Board of the Member.

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

v. **'Specified Members'** shall conduct DR drills/live trading from the DR site on **half yearly basis**. DR drills/ live trading shall include running all operations from DRS for at least **1 full trading day**.

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

vii. Hardware, system software, application environment, network and security devices, and associated application environments of DRS and PDC shall

have a one-to-one correspondence between them. Adequate resources shall be always made available to handle operations at PDC or DRS.

viii. The **Recovery Time Objective (RTO)** i.e., the maximum time taken to restore operations of **'Critical Systems'** from DRS after the declaration of '**Disaster'** shall be **2 Hours** and, **Recovery Point Objective (RPO)** i.e., the maximum tolerable period for which data might be lost due to a major incident shall be **15 Minutes**.

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

x. The BCP-DR policy document shall be reviewed at least **once a year** to minimize incidents affecting business continuity. Additionally, an Adhoc review of the BCP-DR policy shall also be conducted in case of any major changes in **'Critical Systems'** and if any technical glitch is encountered. The BCP-DR policy document of the Members should be approved by Governing Board of the Members.

xi. The Governing Board of the Members shall review the implementation of BCPDR policy approved by the Governing board of the Members on a Quarterly basis. Further, Members 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.

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

xiii. The **'Specified Members'** shall constitute an Incident and Response Team (IRT) / Crisis Management Team (CMT), which shall be chaired by the Managing Director (MD) of the Member 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 Members as part of BCP-DR Policy Document.

xiv. In addition to the above, **'Specified Members'** shall obtain **ISO27001** (Information Security) certification within the 2 years, from April 1, 2023. Additionally, **ISO20000** (IT Service Management) and **ISO22301** (Business Continuity Management System) are recommended to be adhered to. All Policies procedures and processes must be based on these international Standards.

Penalty / Disciplinary Action

Sr. No.	Instances of technical glitches	Financial disincentives	
		Specified Members	**All other Members**
1.	**Technical Glitch continuing for <u>more than 15 minutes</u>:**		
	First instance	Observation Letter	Observation Letter
	Second instance	Administrative warning	Administrative warning
	Third instance onwards	For every instance Rs. 50,000/- It will progressively increase by Rs.25,000/- for subsequent instances. Additionally, the relevant authority of the Exchange on a case-to-case basis and based on the gravity of noncompliance shall decide on additional disciplinary actions.	For every instance Rs. 20,000/- It will progressively increase by Rs.5,000/- for subsequent instances. Additionally, the relevant authority of the Exchange on a case-to-case basis and based on the gravity of noncompliance shall decide on additional disciplinary actions.
2.	**More than 5 Technical Glitch Incidents during the financial year.** **(Incidents lasting more than 15 minutes**)	In addition to the penalty already levied as per the above provisions, no onboarding of new clients till stock exchange analyses RCA and satisfies itself about corrective measures taken or, 15 days from glitch whichever is higher. Additionally, the relevant authority of the Exchange on a case-to-case basis and based on the gravity of noncompliance shall decide on additional disciplinary actions.	The relevant authority of the Exchange on a case-to-case basis and based on the gravity of non-compliance shall decide on the disciplinary actions.
3.	**Failure to restore operations by moving to DR site within**	Rs.2 lac	Rs. 20,000/-

Additionally, RCA reports for all technical glitch incidents greater than 45 minutes, shall also be verified by an independent auditor appointed by the Member.

Trading Members are required to submit Root Cause Analysis (RCA) Report of the technical glitch to the Exchange, within 14 days from the date of the incident. Furthermore, in the case of technical glitch incidents lasting more than 45 minutes, an independent auditor's report on the RCA shall be submitted within 45 days of the incident

Circulars for reference

Issued by	**Circular Dated**	**Circular No**	**Particulars**
SEBI	July 05, 2021	SEBI/HO/MRD1/DTCS/CIR /P/2021/590	Standard Operating Procedure for handling of technical glitches by Market Infrastructure Institutions (MIIs) and payment of "Financial Disincentives" thereof
MCX	December 15, 2021	MCX/TECH/774/2021	Guidelines on Technical Glitches to prevent any business disruption
SEBI	November 25, 2022	SEBI/HO/MIRSD/TPD-1/P/CIR/2022/160	Framework to address the 'technical glitches' in Stock Brokers' Electronic Trading Systems
MCX	December 02, 2022	MCX/TECH/694/2022	Framework to address the 'Technical Glitches' in Stock Brokers' Electronic Trading Systems
MCX	December 16, 2022	MCX/TECH/726/2022	Framework to address the 'technical glitches' in Member's Electronic Trading Systems
MCX	March 10, 2023	MCX/TECH/164/2023	Identification of Specified Members for the framework on 'Technical Glitches'
MCX	January 03, 2024	MCX/TECH/004/2024	Addendum to Framework to address the 'technical glitches' in Member's Electronic Trading Systems

CHAPTER 6

Artificial Intelligence (AI) and Machine Learning (ML) applications

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.

There is increasing usage of AI (Artificial Intelligence) and ML (Machine Learning) as product offerings by market intermediaries and participants (e.g.: “robo advisors”) in investor and consumer facing products. 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.

As most AI / ML systems are black boxes and their behavior cannot be easily quantified, it is imperative to ensure that any advertised financial benefit owing to these technologies in investor facing financial products offered by intermediaries should not constitute to misrepresentation.

Scope definition

Any set of applications / software / programs / executable / systems (computer systems) – cumulatively called application and systems,

- that are offered to investors (individuals and institutions) by market intermediaries to facilitate investing and trading, OR
- to disseminate investments strategies and advice, OR
- to carry out compliance operations / activities,

  where AI / ML is portrayed as a part of the public product offering or under usage for compliance or management purposes, is included in the scope of this circular. Here, “AI” / “ML” refers to the terms “Artificial Intelligence” and “Machine Learning” used as a part of the product offerings. 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 market participants that involves AI and ML
- Technologies that are considered to be categorized as AI and ML technologies in the scope of this circular, are explained in Annexure B of SEBI circular.

Regulatory requirements

- All registered Stock Brokers / Depository Participant offering or using applications or systems as defined in Annexure 16 of SEBI circular, should participate in the reporting process by completing the AI / ML reporting form, mentioned as **Annexure 10**

- As per communication received from SEBI, members are hereby informed that timeline for reporting of Artificial Intelligence (AI) and Machine Learning (ML) applications and systems shall be revised and the below mentioned timelines will be followed with immediate effect:

Intermediary	Current Timeline for reporting of AI/ML applications	Revised Timeline for reporting of AI/ML applications
Trading Members using Algorithm software	Quarterly basis within 15 calendar days of the expiry of the quarter	Half yearly basis within 15 calendar days of the expiry of the half year
Other Trading Members		Annually within 15 calendar days of the expiry of a year

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 it subsequent execution steps on these parameters.
6. A system that does knowledge representation and maintains a knowledge base.

Non-compliant members shall render themselves liable for action as may be deemed fit by the Exchange.

Circulars for Reference

Issued by	Circular Dated	Circular No	Particulars
SEBI	January 11, 2019	SEBI/HO/MIRSD/DOS2/CIR/P/2019/10	Reporting for Artificial Intelligence (AI) and Machine Learning (ML) applications and systems offered and used by market intermediaries
MCX	January 11, 2019	MCX/INSP/014/2019	Reporting for Artificial Intelligence (AI) and Machine Learning (ML) applications and systems offered and used by market intermediaries
MCX	December 22, 2023	MCX/TECH/925/2023	Change in submission timeline for reporting of Artificial Intelligence (AI) and Machine Learning (ML) applications and systems offered and used by market intermediaries

CHAPTER 7

Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs)

In recent times, the dependence on cloud computing for delivering the IT services is increasing. While cloud computing offers multiple advantages viz. ready to scale, ease of deployment, no overhead of maintaining physical infrastructure etc., the RE should also be aware of the new cyber security risks and challenges which cloud computing introduces.

Please refer to below mentioned circular for detailed guidelines.

Format for Submission of Details of Cloud Deployments is enclosed as **Annexure 11**

Circulars for Reference

Issued by	Circular Dated	Circular No	Particulars
SEBI	March 06, 2023	SEBI/HO/ITD/ITD_VAPT/P/CIR /2023/033	Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs)
MCX	March 09, 2023	MCX/TECH/158/2023	Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs)

CHAPTER 8

Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions

Under guidance received from SEBI as per circular no. SEBI/HO/MIRSD2/DOR/CIR/P /2020/221 dated November 03, 2020 & subsequent Amber advisory from CERT-In – 201155100308, Members have to confirm that whether specified confidential data and data types (as specified in the CERT-In advisory) are hosted/ not hosted on SaaS provider/ use or does not use any SaaS based GRC solutions on half yearly basis as per the prescribed format.

In this regard, Indian Computer Emergency Response Team (CERT-in) has issued an advisory for Financial Sector organizations. Please refer the below circular for details advisory.

It is advised to ensure complete protection and seamless control over the critical systems at your organizations by continuous monitoring through direct control and supervision protocol mechanism while keeping the critical data within the legal boundary of India.

The compliance of the advisory shall be reported in the half yearly report by stock brokers and DP to stock exchanges and depositories respectively and by direct intermediaries to SEBI with an undertaking, "Compliance of the SEBI circular for Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions has been made."

Format to submit the SaaS details is attached as **Annexure 12**

Periodicity of SaaS	Report Submission Period
January – June	July 1 to August 31
July - December	January 1 to February 28

Circulars for Reference

Issued by	Circular Dated	Circular No	Particulars
SEBI	Nov 03, 2020	SEBI/HO/MIRSD2/DOR/CIR /P/2020/221	Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions
MCX	May 25, 2021	MCX/TECH/313/2021	Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions - Revised
MCX	July 19, 2022	MCX/TECH/430/2022	Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions

CHAPTER 9

Advisory for SEBI Regulated Entities (REs) regarding Cybersecurity best practices

This advisory should be read in conjunction with the applicable SEBI circulars (including but not limited to Cybersecurity and Cyber Resilience framework, Annual System Audit framework, etc.) and subsequent updates issued by SEBI from time to time.

The compliance of the advisory shall be provided by the REs along with their cybersecurity audit report (conducted as per the applicable SEBI Cybersecurity and Cyber Resilience framework). The compliance shall be submitted as per the existing reporting mechanism and frequency of the respective cybersecurity audit

As per the advisory Regulated Entities/Trading Members are required to submit the compliance with cyber security audit which is effective with immediate effect.

In consultation with other Exchanges, enclosed Compliance Report has been prepared, refer **Annexure-13**, where, all the Trading Members are required to submit Compliance Letter with sign and stamp to the Exchange.

Circulars for reference

Issued by	**Circular Dated**	**Circular No**	**Particulars**
SEBI	Feb 22, 2023	SEBI/HO/ITD/ITD_VAPT/P/CIR /2023/032	Advisory for SEBI Regulated Entities (REs) regarding Cybersecurity best practices
MCX	May 22, 2023	MCX/TECH/332/2023	Submission of Compliance Letter - Advisory for SEBI Regulated Entities (REs) regarding Cybersecurity best practices

Annexure 1
System Audit Annexures

Details of Auditor

Particulars	**Details**
Name of Auditor	
Auditor Membership No	
Auditor Firm Name	
Email Address	
Auditor Firm Registration No.	
Registered Address	
Contact number	
Auditor Qualification CISA / DISA / CISM / CISSP	
Certification Number	
Regulatory Action against Auditor / Partner / Director	(Yes / No)

Annexure 2

Terms of Reference for System Audit

Audit TOR Clause	Details
1	**System Control and Capabilities**
1(a)	**Order Tracking** The system auditor should verify system process and controls at API based terminals (CTCL / SOR/ IBT / STWT / ALGO / DMA etc.) with regard to order entry, capturing of IP address of order entry terminals, modification / deletion of orders, status of the current order/outstanding orders and trade confirmation.
1(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..
1(c)	**Rejection of orders** Whether system has capability to reject orders which do not go through order level validation at the end of the stockbroker CTCL / IBT / SOR/ STWT / ALGO / DMA etc. and at the servers of Exchange.
1(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.
1(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. - Whether System has settings to restrict / allow the facility to place orders in pro account from a CTCL Terminal. - Whether there is a proper process for enabling the facility of placing orders in pro account from approved location through a CTCL terminal.

1(f)	**Order type distinguishing capability** Whether system has capability to distinguish the orders originating from CTCL / IBT / STWT / ALGO / DMA/SOR etc. Whether CTCL / IBT / STWT / ALGO / DMA / SOR etc. orders are having unique flag/ tag as specified by the Exchange and systems identify the orders emanating from CTCL / IBT / STWT/ALGO/ DMA/SOR etc. by populating the 15-digit CTCL field in the order structure for every order. Whether Broker is using similar logic/ priorities as used by Exchange to treat CTCL / IBT / WT /DMA /SOR etc. client orders.
1(g)	**The installed CTCL system parameters are as per Exchange norms:** • Approved CTCL / IBT / STWT / ALGO / DMA / SOR etc. • Software Name and Version No (as applicable) and • Strategy Name & Version No. • Software developed by • Order Gateway Version • Risk Administration / Manager Version • Front End / Order Placement Version • Provide address of the CTCL / IBT / DMA / SOR / STWT/ ALGO server location (as applicable).
1(h)	**The installed system (viz. CTCL/ IBT / STWT / SOR / DMA / SOR system) features are as prescribed by the Exchange.** **<u>Main Features:</u>** **Price Broadcast** The system has a feature for receipt of price broadcast data. **Order Processing:** The system has a feature which allows order entry and confirmation of orders. The system has a feature which allows for modification or cancellation of orders placed. **Trade Confirmation** The system has a feature which enables confirmation of trades. The system has a feature which provides history of trades for the day to the user.

1(i)	**Execution of Orders / Order Logic Execution of Orders / Order Logic:** The installed system provides a system-based control facility over the order input process. **Order Entry** The system has order placement controls that allow only orders matching the system parameters to be placed. **Order Modification** The system allows for modification of orders placed. **Order Cancellation** The system allows for cancellation of orders placed. **Order Outstanding Check** The system has a feature for checking the outstanding orders i.e., the orders that have not yet traded or partially traded.
1(j)	The installed system (viz. CTCL/ IBT / DMA / SOR / STWT system) parameters are as per Exchange norms. Gateway Parameters • • Trader ID • Market Segment - CM • • CTCL ID • • IP Address • • Exchange Network • • VSAT ID • Leased Line ID • Market Segment – F&O • • CTCL ID • • IP Address • • Exchange Network • • VSAT ID

	• • Leased Line ID • Market Segment – CDS • • CTCL ID • • IP Address • • Exchange Network • VSAT ID • Leased Line ID • Market Segment – CO • • CTCL ID • • IP Address • • Exchange Network • • VSAT ID • Leased Line ID
1(k)	**Trades Information** The installed CTCL system provides a system-based control facility over the trade confirmation process the Trade Confirmation and Reporting Feature: The system should allow confirmation and reporting of the orders that have resulted in trade. The system has a feature which provides history of trades for the day to the user.
2	**Software Change Management – The system auditor should check whether proper procedures have been followed and proper documentation has been maintained for the following:**
2(a)	Processing / approval methodology of new feature request, change or patches
2(b)	Change Management Process, related approvals, Version Control- History, etc. **Change requests:**

	whether the changes are tested before being approved for deployment into production. Whether the categorization of the change is done properly.
2(c)	Fault reporting / tracking mechanism and process for resolution
2(d)	Testing of new releases / patches / modified software / bug fixes
2(e)	Does demonstratable segregation exists between Development / Test / Production environment. The System Auditor to check whether adequate mechanism to restore their trading systems to 'production state' at the end of testing session to ensure integrity of trading system.
2(f)	New release in production – promotion, release note approvals
2(g)	Production issues / disruptions reported during last year, reasons for such disruptions and corrective actions taken.
2(h)	User Awareness
2(i)	The system auditor should check whether critical changes made to the CTCL / IBT / STWT / ALGO / DMA /SOR etc. are well documented and communicated to the Stock Exchange.
2(j)	**Change Management** To ensure system integrity and stability all changes to the installed system are planned, evaluated for risk, tested, approved, and documented. Has the organization implemented a change management process to avoid risk due to unplanned and unauthorized changes for all the information security assets (Hardware, software, network, application). Does the process at the minimum include the following. Planned Changes Are changes to the installed system made in a planned manner. a) Are they made by duly authorized personnel. b) Risk Evaluation Process c) Is the risk involved in the implementation of the changes duly factored in. Change Approval Is the implemented change duly approved and process documented. Pre-implementation process Is the change request process documented. Change implementation process

	Is the change implementation process supervised to ensure system integrity and continuity. Post implementation process Is user acceptance of the change documented. Emergency Changes In case of emergency changes, are the same duly authorized and the manner of change documented later. Are Records of all change requests maintained. Are periodic reviews conducted for all the changes which were implemented.
2(k)	**Patch Management** Does the organization have a documented process/procedure for timely deployment of patches for mitigating identified vulnerabilities. Whether version and patch management controls are in place. Does the organization periodically update all assets including Servers, OS, Database, Middleware, Network Devices, Firewalls, IDS /IPS Desktops etc. with latest applicable versions and patches.
2(l)	**SDLC - Application Development & Maintenance** In case of members self-developed system SDLC documentation and procedures if the installed system is developed in-house.
2(m)	**SDLC - Application Development & Maintenance** Does the organization have any in house developed applications. If yes, then does the organization have a documented process/framework to include processes for incorporating, testing, and providing sign-off for information risk requirements at various stages of Software Development Life Cycle (SDLC). Does the SDLC framework incorporate standards, guidelines, and procedures for secure coding. Are roles and responsibilities clearly defined for various stakeholders in the SDLC framework. Are Application development, Testing (QA and UAT) and Production environments segregated.

2(n)	Changes undertaken pursuant to a change to the stock Exchanges trading system.
2(o)	The auditor should check that stockbrokers are not using software without requisite approval of stock Exchange and there has not been any unauthorized change to the approved software.
3	**Risk Management System (RMS)**
3(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 CTCL terminals (CTCL / IBT/ST WT / ALGO/SOR).
3(b)	**Trading Limits** Whether a system of pre-defined limits / checks such as Single Order Quantity and Single Order Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order value Limit, Order Price limit, spread order quantity and value limit, Cumulative open order value check (unexecuted orders) is 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.
3(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.
3(d)	**Order Review** Whether the system has capability to facilitate review of such orders that were not validated by the system.
3(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 exceed corresponding margin availability of clients. Whether deviations from such pre-defined limits are captured by the system, documented and corrective steps taken.

3(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(g)	**Order Reconfirmation Facility** The installed CTCL system provides for reconfirmation of orders which are larger than that as specified by the member's risk management system. The system has a manual override facility for allowing orders that do not fit the system-based risk control parameters
3(h)	**Settlement of Trades** The installed CTCL system provides a system-based reports on contracts, margin requirements, payment, and delivery obligations. Margin Reports feature should allow for the reporting of client wise / user wise margin requirements as well as payment and delivery obligations.
3(i)	**Information Risk Management** Has the organization implemented a comprehensive integrated risk assessment, governance, and management framework. Has the organization developed detailed risk management program that incorporates standards, guidelines, templates, processes, risk catalogues, checklist, measurement metrics and calendar to support and evidence risk management activities. If yes, is the risk management program calendar reviewed periodically. Are the risk identification and assessment processes repeated periodically to review existing risks and identify new risks. Are risks reported to the Senior Management through reports and dashboards on a periodic basis. Are evidences available to demonstrate risk decisions such as Risk Mitigation, Risk Acceptance, Risk Transfer, Risk Avoidance by senior management. Is there a dedicated Risk Management Team for managing Risk and Compliance activities. Is the Risk Management Framework automated.

	Are SLAs defined for all risk management activities. Has the organization defined procedure/process for Risk Acceptance. Are reports and real time dashboards published in order to report/track Risks.
3(j)	Has the organization deployed alert mechanism for detecting malfunctioning of device, software, and backup system.
4	**Algorithmic Trading - The system auditor should check whether proper procedures have been followed and proper documentation has been maintained for the following:**
4(a)	**Change Management** Whether any changes (modification/addition) to the approved Algos were informed to and approved by the exchange. The inclusion / removal of different versions of Algos should be well documented. Whether only approved strategy and software is used for the trading purpose
4(b)(a)	**Online Risk Management capability** The ALGO server have capacity to monitor orders / trades routed through Algo trading and have online risk management for all orders through Algorithmic trading. The system has functionality for mandatorily routing of orders generated by algorithm through the automated risk management system and only those orders that are within the parameters specified in the risk management systems are allowed to be released to exchange trading system. The risk management system may have following risk controls functionality and only algorithm orders that are within the parameters specified by the risk management systems are allowed to be placed.
4(b)(a)(i)	**Individual Order Level:** Quantity Limits / Maximum Order Size.
4(b)(a)(ii)	Daily Price Range checks
4(b)(a)(iii)	Trade price protection checks Orders shall not be released in breach of the bad trade price for the security in respective segment. System Auditor shall refer relevant MCX circulars with respect to “Pre-Trade risk controls - Market Price Protection” and “Pre-Trade risk controls - Limit Price Protection”.

	System auditor shall verify these checks which are designed to reduce excessive order rejections due to LPP and normally order placement is within the ranges as prescribed by Exchange circulars.
4(b)(a)(iv)	Order Value Checks (Order should not exceed the limit specified by the Exchange) The order value check should be within the ranges as prescribed by Exchange circulars.
4(b)(a)(v)	Market price protection (The pre-set percentage of LTP shall necessarily be accompanied by a limit price) Members are required to adhere to the Market Price Protection check, by not placing any algorithmic orders on the Exchange as a market order. System Auditor shall refer relevant MCX circulars with respect to “Pre-Trade risk controls - Market Price Protection”. System auditor shall verify these checks which are designed to ensure that order placement is within the ranges as prescribed by Exchange circulars.
4(b)(a)(vi)	Spread order Quantity and Value Limit
4(b)(a)(vii)	For all checks in Individual Order Level, Trading Members (TM) are required to maintain a policy which shall be approved by the Board/All partners / Proprietor of the Trading Member.
4(b)(b)(i)	**Client Level:** Cumulative Open Order Value check
4(b)(b)(ii)	Automated Execution check
4(b)(b)(iii)	Net position v/s available margins
4(b)(b)(iv)	Market-wide Position Limits (MWPL) violation checks
4(b)(b)(v)	Position limit checks
4(b)(b)(vi)	Trading limit checks
4(b)(b)(vii)	Exposure limit checks at individual client level and at overall level for all clients
4(b)(b)(viii)	Branch value limit for each branch ID
4(b)(b)(ix)	Security wise limit for each user ID
4(b)(b)(x)	Identifying dysfunctional algorithms
4(b)(b)(xi)	Does system have functionality to specify values as unlimited for any risk controls listed above.

4(b)(b)(a)(i)	Does the member have additional risk controls / policies to ensure smooth functioning of the algorithm. (If yes, please provide details) Immediate or cancel orders are not permitted for Commodity Derivative Segment
4(b)(b)(a)(ii)	As a part of the 13 checks mentioned in the MCX operation master circular, Exchange would like to reiterate trading members should adhere to the Market Price Protection check, by not placing any algorithmic orders on the Exchange as a market order. .
4(b)(b)(a)(iii)	All orders generated by Algorithmic trading product adheres to the permissible limit of orders per second, if any as may be specified by SEBI /Exchange. In case any NNF ID not tagged as Algo and is sending excessive order messages the same should also be checked and validated. System Auditor should check whether NNF IDs are properly tagged or not.
4(c)(i)	**Risk Parameters Controls** The system should allow only authorized person to set the risk parameter. The system auditor should verify the process for any change in Risk Parameters. check whether changes are being done only by Authorised person with proper validation/re-confirmation.
4(c)(ii)	The System should also maintain a log of all the risk parameter changes made. The integrity of all such logs is maintained, in other words logs should not be tampered. System auditor should verify & conduct audit of logs maintained for all modifications in Risk Parameters.
4(c)(iii)	For Risk Parameters Controls Trading Members (TM) are required to maintain a policy along with authorization for any change, validation/modification by Authorised person. The said policy shall be approved by the Board/All partners / proprietor of the Trading Member.
4(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.
4(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 or amounting to dysfunctional algo. The system should be capable to account for all execute, unexecuted and unconfirmed orders, placed by it before releasing further order(s). The system should have pre-defined parameters for an automatic stoppage in the event of algo leading to a loop or a runaway situation.
4(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. The system auditor should verify that stockbroker is not using co-location/co-hosting facility in Commodity Derivatives Segment. The system auditor should verify that stockbroker is not using Algorithmic trading from Exchange Hosted CTCL terminals in Commodity Derivatives Segment. Auditor should ensure that Commodity Derivatives trading is not done from Algo / Co-location facility
4(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. ii. Whether the records of control parameters, orders, traders, and data emanating from trades executed through algorithmic trading are preserved/ maintained by the Stockbroker. v. Whether changes to the control parameters have been made by authorized users as per the Access Matrix. v. 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. vi. Whether the system captures the IP address from where the Algo orders are originating.

4(h)	**Systems and Procedures** The system auditor should check and comment on the procedures, systems, and technical capabilities of stockbroker 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. Whether installed systems & procedures are adequate to handle algorithm orders/ trades. The system auditor should also identify any misuse or unauthorized access to algorithms or the system which runs these algorithms. Whether details of users activated for algorithm facilities is maintained along with username, unique identification of user, authorization levels. Does the organization follow any other policy or procedures or documented practices that are relevant.
4(i)	**Reporting to Stock Exchanges** The system auditor should check whether the stockbroker is informing the stock exchange regarding any incidents where the Algo has not behaved as expected. The system auditor should also comment upon the time taken by the stockbroker to inform the stock exchanges regarding such incidents. (Applicable for Commodity Derivatives segment). The system auditor should check whether stockbroker make half yearly review of effect of approved strategies on liquidity and has surrender any such strategy which fails to induct liquidity. (Applicable for Commodity Derivatives segment).
4(j)	**Mock Testing or simulation testing** Have all approved Strategies for Algo trading, irrespective of the algorithm having undergone change or not, participated in the mock trading sessions or simulation minimum once a month.
4(k)	**Approved Strategy** Whether Members are placing Algo orders using only approved strategies. Whether all orders are with valid and approved strategy ID allocated by the Exchange.

4(l)	**Liquidity Infusion** Whether approved strategies not taking away liquidity from the market. Whether approved strategies are conducive to efficient price discovery or fair play in the market.
4(m)	**Other Controls** Immediate or Cancel Orders are not permitted in Commodity Derivatives Segment using ATF. Market orders shall not be allowed to be placed in the Commodity Derivatives Segment using ATF and only Limit Order should be placed using ATF. All orders generated by Algorithmic trading products adhere to the permissible limit of orders per second, if any, as may be specified by SEBI/Exchange. Whether algorithm orders have unique flag/ tag as specified by the Exchange. All orders generated from algorithmic system are tagged with a unique identifier – 13th digit of CTCL field is populated as per published API.
4(n)	**The risk management system has the following model risk controls** 1. Circuit Breaker Check 2. Market Depth Check 3. Last Price Tolerance (LPT) Check 4. Fair Value Check
4(o)	Whether member has submitted undertaking to the Exchange for performance / return claimed by unregulated platforms offering algorithmic strategies for trading as per SEBI circular no. SEBI/HO/MIRSD/DOP/P/CIR/2022/117 dated September 02, 2022, and member is not in violation in this regard.
5	**Password Security**
5(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 API based terminals (CTCL terminals).
5(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.

5(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..
5(d)	The installed CTCL Facility system Authentication mechanism is as per the guidelines of the Exchange. The installed CTCL/IBT/DMA/SOR/STWT/ALGO system used password for authentication. The password policy/standard is documented. The installed systems password features include: a) The installed system uses passwords for authentication. b) The system requests for identification and new password before login into the system. c) The Password is masked at the time of entry. System authenticates user with a Username and password as first level of security. System mandates changing of password when the user logs in for the first time. Automatic disablement of the user on entering erroneous password on five consecutive occasions. The system provides for automatic expiry of passwords at the end of a reasonable duration (maximum 90 Days) and re-initialization of access on entering fresh passwords. Prior intimation is given to the user before such expiry. System controls to ensure that the password is alphanumeric (preferably with one special character), instead of just being alphabets or just numerical. System controls to ensure that the changed password cannot be the same as of the last 6 passwords. System controls to ensure that the Login id of the user and password should not be the same. System controls to ensure that the password should be of minimum six characters. User/Client is deactivated if the same is not used for a continuous period of 12 (Twelve) months from date of last use of the account.

	System allows user to change their passwords at their discretion and frequency. System controls to ensure that the password is encrypted at member's end so that employees of the member cannot view the same at any point of time.
6	**Session Management** **(Mobile Application / Applicability Client Server Application / Web Application)**
6(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.
6(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 WT only.
6(c)	**Inactive Session** Whether the system allows for automatic trading session logout after a system defined period of inactivity.
6(d)	**Log Management** Whether the system generates and maintain logs of Number of users, activity logs, system logs, Number of active clients.
6(e)	The installed system has provision for security, reliability, and confidentiality of data through use of encryption technology, SSL or similar session confidentiality protection mechanisms: a) The system uses SSL/TLS or similar session confidentiality protection mechanisms. b) The system uses a secure storage mechanism for storing usernames and passwords. c) The system adequately protects the confidentiality of the user's trade data.
6(f)	**Cryptographic Controls** Does the organization have a documented process/framework for implementing cryptographic controls in order to protect confidentiality and

	integrity of sensitive information during transmission and while at rest, using suitable encryption technology. Is the encryption methodology of information involved in business transactions based on Regulation/Law/Standards compliance requirements. Does the organization ensure Session Encryption for internet-based applications including the following. Does the organization ensure that the data transferred through internet is protected with suitable encryption technologies. Are transactions on the website suitably encrypted.
6(g)	Cryptographic Controls Is secret and confidential information sent through e-mails encrypted before sending. Is secret and confidential data in an encrypted format.
6(h)	Does the organization have deployed data loss prevention (DLP)solutions / processes.
7	**Database Security**
7(a)	**Access** Whether the system allows CTCL - database access only to authorized users / applications.
7(b)	**Controls** Whether the CTCL database server is hosted on a secure platform, with Username and password stored in an encrypted form using strong encryption algorithms.
7(c)	Data at rest is encrypted
8	**Network Integrity**
8(a)	**Seamless connectivity** Whether stockbroker has ensured that a backup network link is available in case of primary link failure with the exchange.
8(b)	**Network Architecture** Whether the web server is separate from the Application and Database Server.
8(c)	**Firewall Configuration** Whether appropriate firewall is present between stockbrokers trading setup and various communication links to the exchange.

	Whether the firewall default configuration settings are changed and is appropriately configured to ensure maximum security.
8(d)	**Network Security** Are networks segmented into different zones as per security requirements. Are network segments and internet facing assets protected with Intrusion detection/prevention system (IDS/IPS) and/or Firewall to ensure security. Has the organization implemented appropriate monitoring tools to monitor network traffic both within and originating from the organization's network. Does the organization periodically conduct Network Architecture Security assessments in order to identify threats and vulnerabilities. Are the findings of such assessments tracked and closed. Are Internet facing servers placed in a DMZ and segregated from other zones by using a firewall. Is there segregation between application and database servers. Are specific port/service accesses granted on firewall by following a proper approval process. Are user and server zones segregated. Are specific port/service accesses granted on firewall by following a proper approval process. Are the rules defined in the firewall adequate to prevent unauthorized access to IBT/DMA/STWT
9	**Access Controls**
9(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.
9(b)	**Additional Access controls** Whether the system provides for any authentication/two factor authentication mechanism to access to various components of the CTCL terminals (CTCL / IBT/ STWT / ALGO) respectively. Whether additional password requirements are set for critical features of the system. Whether the access control is adequate.
9(c)	**Access Control** Does the organization’s documented policy and procedure include the access control policy.

	Is access to the information assets based on the user's roles and responsibilities. Does the system have a password mechanism which restricts access to authenticated users. Does the system request for identification and new password before login into the system. Does the system have appropriate authority levels to ensure that the limits can be setup only by persons authorized by the risk / compliance manager. Does the organization ensure that access control between website hosting servers and internal networks is maintained. Are records of all accesses requested, approved, granted, terminated, and changed maintained. Are all accesses granted reviewed periodically. Does the organization ensure that default system credentials are disabled/locked. Are Application development, Testing (QA and UAT) and Production environments segregated. Whether adequate controls have been implemented for admission of personnel into the server rooms / place where servers / hardware / systems are located and whether audit trails of all the entries/exits at the server room / location are maintained. Is access to the information assets based on the user's roles and responsibilities. Does the system have a password mechanism which restricts access to authenticated users.
9(d)	**Extra Authentication Security** If the systems use additional authentication measures like smart cards, biometric authentication, or tokens etc.
9(e)	**Physical & Environmental Security** Does the organization have a documented process/framework for Physical & Environmental Security. Are adequate provisions in respect of physical security of the hardware / systems at the hosting location and controls on admission of personnel into the location (audit trail of all entries-exits at location etc.). Are security perimeters defined based on the criticality of assets and operations.

	Are periodic reviews conducted for the accesses granted to defined perimeters. Are CCTV cameras deployed for monitoring activities in critical areas. Is the CCTV footage backed up and can it be made available in case the need arises. Are suitable controls deployed for combating fire in Data Center. Does the organization maintain physical access controls for Server Room/Network Room security (environmental controls) Server Room, Network Room Security (UPS), Server room. network room security (HVAC). Are records maintained for the access granted to defined perimeters. Are suitable controls deployed for combating fire in the data center.
9(f)	**Privileged Identity Management** Does the organization have a documented process/procedure for defining reviewing and assigning the administrative roles and privileges. Has the organization implemented controls/tools for Privilege Identity Management including at a minimum provisioning, maintenance, monitoring, auditing, and reporting all the activities performed by privileged users (Sys Admin, DBA etc.) accessing organization's IT systems. Are Privileges granted to users based on appropriate approvals and in accordance with the user's role and responsibilities. Are all the activities of the privileged users logged. Are log reviews of privileged user logs of admin activity conducted periodically. Is Maker- Checker functionality implemented for all changes by admin. Are records of privileged user provisioning/deprovisioning reviewed.
9(g)	**Closed User Group Endpoint Security** Does the member have policies and procedures having coverage related to People, Processes and Technology. Does the broker member have architecture that supports segregation such as Business - stock broking & Other business of stockbroker Data and Processing facilities Development / Test / Production environment Corporate user and Production / server zones Application and Database servers Internet facing servers placed in a DMZ and segregated from other zones Ensure appropriately configured firewalls are used to ensure segregation wherever needed.

	Are technology related Baseline Controls established, exercised, and reviewed periodically. Are following systems and processes existing and exercised for Vulnerability Assessment and Penetration Testing Configuration of Technologies prior to go live Monitoring of perimeter / network security, infrastructure and applications for anomalies alerts incidents and breaches Reporting of cyber-attacks, threats, cyber-incidents and breaches experienced and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities, threats to be submitted to stock exchange and other regulatory agencies based on applicability.
10	**Backup and Recovery**
10(a)	**Backup and Recovery Policy** Whether the organization has a well-documented policy on periodic backup of data generated from the broking operations.
10(b)	**Log generation and data consistency** Whether backup logs are maintained, and backup data is tested for consistency.
10(c)	**System Redundancy** Whether there are appropriate backups in case of failures of any critical system components.
10(d)	**Backup & Restoration** The Installed systems backup capability is adequate as per the requirements of the Exchange for overcoming loss of product integrity. Are backups of the following system generated files maintained as per the Exchange guidelines. At the server/gateway level a) Database b) Audit Trails Reports At the user level a) Market Watch b) Logs c) History d) Reports e) Audit Trails f) Alert logs

	Does the audit trail capture the record of control parameters, orders, trades, and data points emanating from trades executed through algorithm trading. Does the organization ensure that the audit trail data maintained is available for a minimum period of 5 years. Does the organization ensure that the user details including username, unique identification of user, authorization levels for the users activated for algorithm facilities maintained and is available for a minimum period of 5 years. Does the audit trail for SOR capture the record of orders, trades, and data points for the basis of routing decision. Are backup procedures documented and backup logs maintained. Are the backup logs maintained and are the backups verified and tested. Are the backup media stored safely in line with the risk involved. Are there any recovery procedures and have the same been tested. Are the backups restored and tested periodically to ensure adequacy of backup process and successful restoration.
10(e)	**Audit trail, Event logging and monitoring** Members should maintain logs of all trading activity to facilitate audit trail. Whether system generates, captures, and maintains audit trail of all transactions for at least 3 years. Whether Audit trail should capture record of control parameters, orders, trades, and data points emanating from trades executed through algorithmic trading. Whether All events, changes in master, strategy parameters shall be logged and maintained for at least 3 years. Whether all logs generated are secured from unauthorized modifications.

10(f)	How will the organization assure customers prompt access to their funds and securities in the event the organization determines it is unable to continue its business in the primary location - Network / Communication Link Backup. Is the backup network link adequate in case of failure of the primary link to the Exchange. Is the backup network link adequate in case of failure of the primary link connecting the users. Is there an alternate communications path between customers and the firm. Is there an alternate communications path between the firm and its employees. Is there an alternate communications path with critical business constituents, banks, and regulators. Whether detailed network diagram is prepared and available for verification. Is network and network diagram in line with the one submitted to the Exchange. Does the organization have an alternate means of communication including a channel for communication for communicating with the clients in case of any disruption. Such communication should be completed within 30 minutes from the time of disruption.
10(g)	How will the organization assure customers prompt access to their funds and securities in the event the organization determines it is unable to continue its business in the primary location - System Failure Backup Are there suitable backups for failure of any of the critical system components like a) Gateway / Database Server b) Router c) Network Switch **Infrastructure breakdown backup** Are there suitable arrangements made for the breakdown in any infrastructure components like d) Power Supply e) Water f) Air Conditioning **Primary Site Unavailability** Have any provision for alternate physical location of employees been made in case of non-availability of the primary site

	Disaster Recovery Are there suitable provisions for Books and records backup and recovery (hard copy and electronic). Have all mission-critical systems been identified and provision for backup for such systems been made.
11	**BCP/DR** **(Only applicable for Stockbrokers having BCP / DR site)**
11(a)	**BCP / DR Policy** Whether the stockbroker has a well-documented BCP/ DR policy and plan. The system auditor should comment on the documented incident response Exchange procedures and observation on the DR drills conducted by the stockbroker.
11(b)	**Alternate channel of communication** Whether the stockbroker has provided its clients with alternate means of communication including channel for communication in case of a disaster. Whether the alternate channel can authenticate the user after asking for additional details or OTP (One-Time-Password).
11(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.
11(d)	**Connectivity with other FMIs** The system auditor should check whether there is an alternative medium to communicate with Stock Exchanges and other FMIs.
11(e)	**Business Continuity** Does the Organization have a suitable documented Business Continuity or Disaster Recovery or Incident Response process commensurate with the organization size and risk profile to ensure a high degree of availability of the installed system Is there any documentation on Business Continuity / Disaster Recovery / Incident Response. If a BCP/DRP plan exists, has it been tested on a regular basis. Are there any documented risk assessments. Does the installation have a Call List for emergencies maintained.

	Whether redundancy is built at all levels of infrastructure. Whether all critical systems / infrastructures are in HA mode.
11(f)	**Security Incident & Event Management** Does the organization have a documented process/policy for Security Incident & Event Management. Does the organization have a documented process/procedure for identifying Security related incidents by monitoring logs generated by various IT assets such as Operating Systems, Databases, Network Devices, etc. Are all events/incidents detected, classified, investigated, and resolved. Are periodic reports published for various identified Security incidents. Does the organization ensure that the logging facilities and the log information Are protected from tampering and unauthorized access.
11(g)	**Security Incident & Event Management** Is there a dedicated Incident Response Team for managing risk and compliance activities.
11(h)	Business Continuity Does the organization have a Disaster Recovery Site. Are there any documented risk assessments. Does the installation have a Call List for emergencies maintained. Does the organization have robust systems and technical infrastructure in place in order to provide essential facilities, perform systemically critical functions relating to securities market and provide seamless service to their clients.
11(i)	The system auditor should comment on the documented incident response procedures. which will cover the following: Identification of all critical operations of the Member and include the process of informing clients in case of any disruptions. While putting in place the BCP/DR plan, members are advised to sufficiently review all potential risks along with its impact on the business. Declaration of incident as a “Disaster” viz. timelines etc. and restoration of operations from DR Site upon declaration of ‘Disaster’ Adequate resources (with appropriate training and experience) should be available at the DR Site to handle all operations during disasters. The declaration of disaster shall be reported in the preliminary report submitted to the Exchange.

11(j)	Does the organization have distinct primary and disaster recovery sites (DRS) for technology infrastructure, workspace for people and operational processes. Does the organization have DRS set up sufficiently away (not less than 250 km), from Primary Data Centre (PDC) to ensure that both DRS and PDC are not affected by the same disasters. Has any provision for alternate physical location of employees been made in case of non-availability of the primary site Disaster Recovery. Does the organization have suitable provisions for Books and records backup and recovery (hard copy and electronic). Have all mission-critical systems been identified and provision for backup for such systems been made.
12	**Segregation of Data and Processing facilities**
12(a)	The system auditor should check and comment on the segregation of data and processing facilities at the Stockbroker in case the stockbroker is also running other business.
13	**Back-office data**
13(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.
13(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**
14(a)	**User Management Policy** The system auditor should check whether the stockbroker has a well-documented policy that provides for user management and the user management policy explicitly defines user, database, and application Access Matrix.
14(b)	**Access to Authorized users** The system auditor should check whether the system allows access only to the authorized users of the CTCL 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.

14(c)	**User Creation / Deletion** The system auditor should check whether new user ids were created / deleted as per CTCL guidelines of the exchange and whether the user ids are unique in nature.
14(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.
14(e)	**User Management system** User Deletion: Users are deleted as per the Exchange guidelines Reissue of User Ids: User Ids are reissued as per the Exchange guidelines. Locked User Accounts: Users whose accounts are locked are unlocked only after documented unlocking requests are made.
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))**
15(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.
15(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.
15(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

15(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.
15(e)	**Infrastructure High Availability** Does the organization have a documented process for identifying single point of failure. Does the organization have a documented process for failover. Does the organization ensure that various components pertaining to networks, servers, storage have sufficient redundancy. Does the organization conduct periodic redundancy/contingency testing.
15(f)	To ensure information security for the Organization in general and the installed system in particular policy and procedures as per the Exchange requirements must be established, implemented, and maintained. Does the organization's documented policy and procedures include the following policies and if so, are they in line with the Exchange requirements and whether they have been implemented by the organization. Information Security Policy Password Policy User Management and Access Control Policy Network Security Policy Application Software Policy Change Management Policy Backup Policy BCP Management Policy Audit Trail Policy Capacity Management Plan Does the organization follow any other policy or procedures or documented practices that are relevant.
15(g)	**Are documented practices available for various system processes** Day Begins Day Ends **Other system processes** a) Audit Trails b) Access Logs c) Transaction Logs d) Backup Logs e) Alert Logs f) Activity Logs

	g) Retention Period h) Data Maintenance
15(h)	**In case of failure, is there an escalation procedure implemented.** Day Begin Day End Other system processes **Details of the various response procedures including for** a) Access Control failure b) Day Begin failure c) Day End failure d) Other system Processes failure
15(i)	**Vulnerability Assessment, Penetration Testing & Application Security Assessments:** Are periodic vulnerability assessments for all the critical assets including Servers, OS, Database, Middleware, Network Devices, Firewalls, IDS /IPS etc. conducted.
15(j)	**Standards & Guidelines** Does the organization maintain standards and guidelines for information security related controls, applicable to various IT functions such as System Administration, Database Administration, Network, Application, and Middleware etc. Does the organization maintain Hardening Standards pertaining to all the technologies deployed within the organization related to Applications, OS, Hardware, Software, Middleware, Database, Network Devices and Desktops. Does the organization have a process for deploying OS, Hardware, Software, Middleware, Database, Network Devices and Desktops after ensuring that they are free from vulnerabilities. Are the defined standards, guidelines updated and reviewed periodically.
15(k)	**Information Security Policy & Procedure** Do the organizations documented policy and procedures include the information security policy and if so, are they compliant with legal and regulatory requirements. Is the defined Policy & Procedures reviewed on a periodic basis.
15(l)	**Information Security Policy & Procedure** Are any other standards/guidelines like ISO 27001 etc. being followed. Does the organization have an Information Security Forum to provide overall direction to information security initiatives based on business objectives.

15(m)	**Information Classification & Protection** Has the organization defined Systematic and documented framework for Information Classification & Protection. Are the information items classified and protected in accordance with business criticality and sensitivity in terms of Confidentiality, Integrity & Availability. Does the organization conduct periodic information classification process audits. Has the organization deployed suitable controls to prevent leakage of sensitive information.
15(n)	**Vulnerability Assessment, Penetration Testing & Application Security Assessments** Does the organization maintain an annual VAPT and Application Security Assessment activity calendar. Is periodic Router ACL review conducted as a part of Vulnerability Assessment.
15(o)	Does the organization have hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments.
15(p)	**Amazons AWS S3 and EC2 service Controls** Does the organization check public accessibility of all AWS instances in use. Make sure that no server/bucket is inadvertently leaking data due to inappropriate configurations.
15(q)	Does the organization ensure proper security of AWS access tokens. The tokens should not be exposed publicly in website source code, any configuration files etc..
15(r)	Does the organization implement appropriate security measures for production, testing, staging, and backup environments hosted on AWS. Does the organization ensure that production environment is kept properly segregated from these. Does the organization disable/remove older or testing environments if their usage is no longer required.
15(s)	The Apache Software Foundation released an emergency patch as part of the 2.15.0 release of Log4j that fixes the Remote Code Execution (RCE) vulnerability. Does the Organizations Application administrators and developers verify the use of Log4j package in their environment and upgrade to version 2.15.0.

16	**Software Testing Procedures - The system auditor should check whether the stockbroker has complied with the guidelines and instructions of SEBI / stock exchanges with regard to testing of software and new patches, including the following:**
16(a)	**Test Procedure Review** The system auditor should review and evaluate the procedures for system and software/program testing. The system auditor should also review the adequacy of tests.
16(b)	**Documentation** The system auditor should verify whether the documentation related to testing procedures, test data, and resulting output were adequate and follow the organizations standards.
16(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 various SEBI circulars.
17	**Additional Points**
17(a)	**Antivirus Management** Does the organization have a documented process/procedure for Antivirus Management. Are all information assets protected with anti-virus software and the latest anti-virus signature updates. Does the organization periodically perform scans for virus/malicious code on computing resources, email, internet, and other traffic at the Network Gateway/entry points in the IT Infrastructure. Does the organization have a documented process/procedure for tracking, reporting, and responding to virus related incidents.
17(b)	**Anti-virus** Is a malicious code protection system implemented. If yes, then Are the definition files up to date. Any instances of infection. Last date of virus checks of entire system

17(c)	The installed system provides a system based event logging and system monitoring facility which monitors and logs all activities / events arising from actions taken on the gateway / database server, authorized user terminal and transactions processed for clients or otherwise and the same is not susceptible to manipulation. The installed systems has a provision for On-line surveillance and risk management as per the requirements of Exchange and includes Number of Users Logged In / hooked on to the network incl. privileges of each The installed systems has a provision for off line monitoring and risk management as per the requirements of Exchange and includes reports / logs on a) Number of Authorized Users b) Activity logs c) Systems logs d) Number of active clients
17(d)	**Insurance** The insurance policy of the Member covers the additional risk of usage of system and probable losses in case of software malfunction
17(e)	**Firewall** Whether suitable firewalls are implemented. Are the rules defined in the firewall adequate to prevent unauthorized access to IBT/DMA/STWT systems.
17(f)	**Compliance** Does the organization have a documented process/policy implemented to ensure compliance with legal, statutory, regulatory, and contractual obligations and avoid compliance breaches. Does the organization ensure compliance to the following. · IT Act 2000 · Sebi Requirement Does the organization maintain an integrated compliance checklist. Are these defined checklists periodically updated and reviewed to incorporate changes in rules, regulations, or compliance requirements. Whether the order routing servers routing CTCL/ALGO/IBT/DMA/STWT/SOR orders are located in India. Provide address of the CTCL / IBT / DMA / SOR / STWT server location (as applicable).

	Whether the required details of all the CTCL facility user ids created in the server of the trading member, for any purpose (viz. administration, branch administration, mini-administration, surveillance, risk management, trading, view only, testing, etc.) and any changes therein, have been uploaded as per the requirement of the Exchange. If no, please give details. Whether all the CTCL facility user ids created in the server of the trading member have been mapped to 12-digit codes on a one-to-one basis and a record of the same is maintained. If no, please give details. The system has an internal unique order numbering system. All orders generated by CTCL terminals (CTCL/IBT/DMA/STWT/SOR/ALGO) are offered to the market for matching and system does not have any order matching function resulting into cross trades. Whether algorithm orders are having unique flag/ tag as specified by the Exchange. All orders generated from algorithmic system are tagged with a unique identifier – 13th digit of field is populated appropriately. Whether every algorithm order reaching on exchange platform is tagged with the unique identifier allotted to the respective algorithm by the Exchange. All orders routed through CTCL/IBT/STWT/DMA/SOR/ALGO are routed through electronic / automated Risk Management System of the broker to carry out appropriate validations of all risk parameters before the orders are released to the Exchange. The system and system records with respect to Risk Controls are maintained as prescribed by the Exchange which are as follows: The limits are setup after assessing the risks of the corresponding user ID and branch ID. The limits are setup after taking into account the member's capital adequacy requirements. All the limits are reviewed regularly and the limits in the system are up to date. All the branch or user have got limits defined and that No user or branch in the system is having unlimited limits on the above stated parameters. Daily record of these limits is preserved and shall be produced before the Exchange as and when the information is called for. Compliance officer of the member has certified the above in the quarterly compliance certificate submitted to the Exchange.

	IBT/STWT Compliance Does the broker's IBT / STWT system complies with the following provisions. The system captures the IP (Internet Protocol) address (from where the orders are originating), for all IBT/ STWT orders. The system has built-in high system availability to address any single point failure. The system has secure end-to-end encryption for all data transmission between the client and the broker system through a Secure Standardized Protocol. A procedure of mutual authentication between the client and the broker server is implemented. The system has adequate safety features to ensure it is not susceptible to internal/ external attacks. In case of failure of IBT/ STWT, the alternate channel of communication has adequate capabilities for client identification and authentication. Two-factor authentication for login session has been implemented for all orders emanating using Internet Protocol. In case of no activity by the client, the system provides for automatic trading session logout. The back-up and restore systems implemented by the broker is adequate to deliver sustained performance and high availability. 1. The broker system has on-site as well as remote site back-up capabilities Name of the website provided in the application form is the website through which Internet based trading services is to be provided to the clients. 2. Secured socket level security for server access through Internet is available. SSL certificate is valid and trading member is the owner of the website provided. 3. Any change in name of the website or ownership of the website shall be incorporated only on approval from the Exchange. Whether the order routing servers routing CTCL/ALGO/IBT/WT/DMA/SOR orders are located in India and through specified CTCL / ATS User ID approved by the Exchange for Trading ATF software / IDs do not have any interlink with any system or ID located / linked outside India. Whether the required details of all the CTCL user ids created in the server of the trading member, for any purpose (viz. administration, branch administration, mini-administration, surveillance, risk management, trading,

	view only, testing, etc.) and any changes therein, have been uploaded as per the requirement of the Exchange. If no, please give details. Whether all the CTCL user ids created in the server of the trading member have been mapped to 12 digit codes on a one-to-one basis and a record of the same is maintained. If no, please give details. The system has an internal unique order numbering system. All orders generated by CTCL terminals (CTCL/IBT/WT/ALGO) are offered to the market for matching and system does not have any order matching function resulting into cross trades. All orders routed through CTCL / IBT / WT are routed through electronic / automated Risk Management System of the broker to carry out appropriate validations of all risk parameters before the orders are released to the Exchange.
17(g)	**Vendor Certified Network diagram** Date of submission of network diagram to Exchange (Only in case of change in network setup, member needs to submit revised scanned copy network diagram along with this report). Verify number of nodes in diagram with actual Verify location(s) of nodes in the network.
17(h)	**DOS** Has the organization implemented strong monitoring, logging, detection, and analysis capability to detect and mitigate DOS/DDOS attacks. Does the organization have a documented process/procedure/policy defining roles and responsibilities and plan of action in order to deal with DOS/DDOS attacks pro-actively and post the incidence.
17(i)	**DOS** Does the organization periodically conduct mock DOS scenarios to have insight into the preparedness in tackling with DOS/DDOS attacks.

17(j)	**Third Party Information Security Management** Does the organization have a documented process/framework for Third Party Vendor Management including at a minimum process and procedure for on-boarding/off-boarding of vendors, checklist for prescribing and assessing compliance, assessment and audit for both onsite & offsite vendors. Does the organization conducts periodic information security compliance audits/reviews for both onsite and offsite vendors. Are Risks associated with employing third party vendors addressed and mitigated. Is the defined process/framework periodically reviewed.
17(k)	**Capacity Management** Does the organization have documented processes/procedures for capacity management for all the IT assets. Are installed systems & procedures adequate to handle algorithm orders/trades. Is there a capacity plan for growth in place
17(l)	**Independent Audits** Are periodic independent audits conducted by Third Party / internal Auditors. Are the audit findings tracked to closure.
17(m)	**Human Resources Security, Acceptable Usage & Awareness Trainings** Are periodic surprise audits and social engineering attacks conducted to assess security awareness of employees and vendors. Has the organization implemented policy/procedure defining appropriate use of information assets provided to employees and vendors in order to protect these assets from inappropriate use. Are these policies/procedures periodically reviewed and updated. Does the organization perform Background Checks for employees (permanent, temporary) before employment. Does the organization conduct Information Security Awareness Program through trainings and Quiz for employees and vendors.

17(n)	Does the organization display the 'Risk disclosures' given at Annexure-I Circular no SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/73 dated May 19, 2023, on their websites and to all their clients in the manner as specified below: Upon login into their trading accounts with brokers, the clients may be prompted to read the 'Risk disclosures' (which may appear as a pop-up window upon login) and shall be allowed to proceed ahead only after acknowledging the same. The 'Risk disclosures' shall be displayed prominently, covering at least 50 percent area of the screen.
17(o)	Whether a functionality is developed on stock broker's (with retail clients) non-NEAT front end including IBT,STWT,CTCL etc. whereby any person placing an order in a security which is under Graded Surveillance Measure(GSM)/ Additional Surveillance Measure(ASM)/IRP as per IBC/Unsolicited SMS or Videos/Pledge/ASM ICA/ASM IBC etc. gets the message as per Exchange circular, at the time of placing the order and is aware of such surveillance action on the scrip before placing the order. (Not applicable for commodity Exchange)
17(p)	Compliance with Exchange circular Whether the Member has developed the functionality to facilitate dissemination of scrip specific cautionary messages (single/multiple) on trading terminals at the time of order entry (for Buy & Sell both) to identify securities which are under Surveillance and Other actions, on their non-NEAT front end including IBT, STWT, CTCL etc., as per Exchange Circular. Whether any person(client of the Member) while placing an order in a security for which the cautionary indicators are applicable (as per the REG_INDDDMMYY.csv file and 'fo_secban_DDMMYYYY.csv'), gets the following message so that the person placing the order is aware of such single/multiple actions on the scrip before placing the order. In case multiple messages are eligible to be displayed, whether trading members are providing all eligible messages in the pop-up. Whether the Member has included the verbatim of the pop-up message on the trading front-end. (Not applicable for commodity Exchange)
17(q)	Whether the member is complying with the Exchange circular MCX/CTCL/748/2022 dated December 29, 2022, for "Display of Brokerage, Statutory & Regulatory Levies"
17(r)	Whether member is allowing to place orders to only approved FPI clients using DMA facility as specified in as per SEBI/HO/MRD/MRD-RAC-1/P/CIR/2022/131 September 29, 2022 regarding Participation of SEBI registered Foreign Portfolio Investors(FPIs)in Exchange Traded Commodity Derivatives in India and SEBI circular i.e. SEBI/HO/MRD/MRD-PoD-1/P/CIR/2023/68 May 10, 2023 regarding "Direct Market Access(DMA)to

	SEBI registered Foreign Portfolio Investors (FPIs) for participating in Exchange Traded Commodity Derivatives(ETCDs)"
17(s)	**Change Management: (Applicable to COLO Members) -** (Not applicable for commodity Exchange) Any new hardware and software addition/change hosted in COLO (including firmware changes) shall be thoroughly tested during mock or simulation market.
17(t)	**Traffic Monitoring: (Applicable to COLO Members)** (Not applicable for commodity Exchange) The member shall also monitor the traffic originating from Its own IT infrastructure hosted in COLO towards Exchange and put adequate controls to prevent any spurious/unwanted. traffic coming to Exchange.
18	**AI-ML**
18(a)	Are adequate safeguards in place to prevent abnormal behavior of the AI or ML application / System.
18(b)	Has Member reported details of AI/ML to Exchange on a quarterly basis in accordance with SEBI circular SEBI/HO/MIRSD/DOS2/CIR/P/2019/10 dated January 04, 2019.
18(c)	Whether AI / ML systems comply for all above System Audit Checklist points. In case of any observation, please report.
19	**Undertaking/Application for CTCL/IBT/STWT/DMA/SOR**
19(a)	The system has been installed after complying with the various Exchanges circulars issued from time to time. Copy of Undertaking provided regarding the CTCL system as per relevant circulars. Copy of application for approval of Internet Trading, if any. Copy of application for approval of Securities trading using Wireless Technology if any Copy of application for approval of Direct Market Access, if any. Copy of application / undertaking provided for approval of Smart Order Routing (SOR)
20	**Pre-Trade Risk Control**
20(a)	Whether appropriate pre-trade checks, alerts, and controls are built in CTCL facility/ systems such that an alert shall be generated if the user places limit order at a price which is away from prevailing market prices.
21	**Asset Management**

21(a)	Does the organization have a documented process/framework for managing all the hardware & software assets. Does the organization maintain a centralized asset repository. Are periodic reconciliation audits conducted for all the hardware and software assets to confirm compliance to licensing requirements and asset inventory.
22	**Phishing & Malware Protection for IBT / STWT**
22(a)	Has the organization implemented controls/ mechanisms to identify and respond to phishing attempts on their critical websites. Are the organizations' websites monitored for Phishing & Malware attacks. Does the organization have a process for tracking down phishing sites.
23	**Smart order routing (SOR) - The system auditor should check whether proper procedures have been followed and proper documentation has been maintained for the following:**
23(a)	**Best Execution Policy** System adheres to the Best Execution Policy while routing the orders to the exchange. **Destination Neutral** The system routes orders to the recognized stock exchanges in a neutral manner. **Class Neutral** The system provides for SOR for all classes of investors **Confidentiality** The system does not release orders to venues other than the recognized stock Exchange. **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 **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. **Audit Trail** Audit trail for SOR should capture order details, trades and data points used as a basis for routing decision. **Server Location**

	The system auditor should check whether the order routing server is located in India **Alternate Mode** The system auditor should check whether an alternative mode of trading is available in case of failure of SOR Facility
24	**Remote Access Controls**
24(a)	Does the organization have proper remote access policy framework incorporating the specific requirements of accessing the enterprise resources are securely located in the data center from home, using internet connection.
24(b)	For implementation of the concept of trusted machine as end users: Does the organization have categorized the machines as official desktops / laptops and accordingly the same are configured to ensure implementation of solution stack considering the requirements of authorized access.
24(c)	Do the organizations' Official devices have appropriate security measures to ensure that the configuration is not tampered with. Does the organization ensure that internet connectivity provided on all officials are not getting used for any purpose other than the use of remote access to data center resources.
24(d)	Does the organization ensure that if personal devices (BYOD) are allowed for general functions, then appropriate guidelines are issued to indicate positive and negative list of applications that are permitted on such devices. Further, these devices are subject to periodic audit.
24(e)	Does the organization implement various measures related to Multi-Factor Authentication (MFA) for verification of user access to ensure better data confidentiality and accessibility. VPN remote access through MFA also needs to be implemented.
24(f)	Does the organization ensure that only trusted machines are permitted to access the data center resources. Does the organizations Virtual Private Network (VPN) remote login is device specific through the binding of the Media Access Control (MAC) address of the device with the IP address to implement appropriate security control measures.
24(g)	Does the organization have appropriate risk mitigation mechanisms whenever remote access of data center resources is permitted for service providers.
24(h)	For on-site monitoring, the Member, Does the organization implement adequate safeguard mechanisms such as cameras, security guards, nearby co- workers to reinforce technological activities.

24(i)	Does the organizations backup, restore and archival functions work seamlessly, particularly if the users have remote access to internal systems.
24(j)	Does the organization apply only necessary and applicable patches to the existing hardware and software.
24(k)	Does the organization analyze generated alerts and alarms. And take appropriate decisions to address the security concerns. Are the organizations security controls for the Remote Access requirements integrated with the SOC Engine and part of the overall monitoring of the security posture.
24(l)	Does the organization have updated the incident response plan in view of the current pandemic. Does the plan cover following: 1. Increase awareness of information technology support mechanisms for employees who work remotely. 2. Implement cyber security advisories received from SEBI, Exchange, CERT-IN and NCIIPC on a regular basis. 3. Further, all the guidelines developed and implemented during pandemic situation shall become SOPs post Covid-19 situation for future preparedness. 4. Disable use of Macros in Microsoft office
25	**SEBI and Exchange Compliances**
25(a)	Auditor to list all applicable Circulars, Notices, Guidelines, and advisories published by SEBI and Exchanges and mention
25(b)	Adherence to all such Circulars, Notices, Guidelines, and advisories published
25(c)	Reporting adherences based on prescribed periodicity in point **25(b)** above.

NOTE:

1. Some of the CTCL facilities like SOR and co-location may not be applicable,

to Commodity Derivative Exchanges auditor is required to refer related circular for the same.

Specific TOR points pertaining to other than Commodity Derivative Segment to be marked.

as not applicable (NA) With justification.

2. STWT – Consider as WT for Commodity Derivatives segment.

Annexure 3

Cyber Audit Annexure

Details of Auditor

Particulars	**Details**
Name of Auditor	
Auditor Membership No	
Auditor Firm Name	
Email Address	
Auditor Firm Registration No.	
Registered Address	
Contact number	
Auditor Qualification CISA / GSNA / CISM / CISSP	
Certification Number	
Regulatory Action against Auditor / Partner / Director	(Yes / No)

Annexure 4

Cyber Security & Cyber Resilience Audit - Terms of Reference (TOR)

Cyber Security & Cyber Resilience Audit - Terms of Reference (TOR)

Audit TOR Clause	Details
1	**Governance**
1(a)(i)	Whether the Stockbroker has formulated a comprehensive Cyber Security and Cyber Resilience policy document encompassing the framework mentioned in the circular.
1(a)(ii)	In case of deviations from the suggested framework, whether reasons for such deviations, technical or otherwise, are provided in the policy document.
1(a)(iii)	Is the policy document approved by the Board / Partners / Proprietor of the organization.
1(a)(iv)	Whether the policy document is reviewed by the aforementioned group at least annually with the view to strengthen and improve its Cyber Security and Cyber Resilience framework.
1(a)(v)	Policy Approval Date
1(a)(vi)	Policy Version
1(a)(vii)	Policy Approval By
1(b)(i)	Whether the Cyber Security Policy includes the following process to identify, assess, and manage Cyber Security risk associated with processes, information, networks, and systems.
1(b)(ii)	a. 'Identify' critical IT assets and risks associated with such assets.
1(b)(iii)	b. 'Protect' assets by deploying suitable controls, tools, and measures.
1(b)(iv)	c. 'Detect' incidents, anomalies, and attacks through appropriate monitoring tools/processes.
1(b)(v)	d. 'Respond' by taking immediate steps after identification of the incident, anomaly, or attack.
1(b)(vi)	e. 'Recover' from incident through incident management and other appropriate recovery mechanisms.

1(c)	Whether policy / Procedure document refers to best practices from international standards like ISO 27001, COBIT 5, etc., or their subsequent revisions, if any, from time to time.
1(d)	Whether policy document have considered the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organization (NTRO), Government of India (titled 'Guidelines for Protection of National Critical Information Infrastructure') and subsequent revisions, if any, from time to time.
1(e)	Stockbrokers / Depository Participants should designate a senior official or management personnel (henceforth, referred to as the "Designated Officer") whose function would be to assess, identify, and reduce security and Cyber Security risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the Cyber Security Policy.
1(f)(i)	Whether the Member has constituted a Technology Committee comprising experts.
1(f)(ii)	This Technology Committee has reviewed on a half yearly basis the implementation of the Cyber Security and Cyber Resilience policy, which includes:
1(f)(iii)	- review of their current IT and Cyber Security and Cyber Resilience capabilities,
1(f)(iv)	- if committee has set goals for a target level of Cyber Resilience and establish plans to improve and strengthen Cyber Security and Cyber Resilience.
1(f)(v)	- And the review report is placed before the Board / Partners / Proprietor of the Stockbrokers / Depository Participants for appropriate action.
1(g)	Whether the Designated officer and the technology committee periodically reviewed instances of cyber-attacks, if any, domestically and globally, and taken steps to strengthen Cyber Security and cyber resilience framework.
1(h)	Whether Brokers / Depository Participants has policy or reporting procedure to facilitate communication of unusual activities and events to the Designated Officer in a timely manner.
1(i)	Has Stockbroker/Depository Participant defined and documented roles and responsibilities of its employees, outsourced staff, and employees of vendors, members or participants and other entities, who may have privileged access or use systems / networks of the Stockbroker/Depository Participants towards ensuring the goal of Cyber Security.

1(j)	Stockbrokers / Depository Participants should prepare detailed incident response plan and define roles and responsibilities of Chief Information Security Officer (CISO) and other senior personnel. Reporting and compliance requirements shall be clearly specified in the security policy. In addition, share the details of CISO with CERT-In through Email (info AT cert-in.org.in)
2	**Identification**
2(a)	Has the Stockbroker / Depository Participant identified and classified critical assets based on their sensitivity and criticality for business operations, services and data management. The critical assets shall include business critical systems, internet facing applications /systems, systems that contain sensitive data, sensitive personal data, sensitive financial data, Personally Identifiable Information (PII) data, etc. All the ancillary systems used for accessing/communicating with critical systems either for operations or maintenance shall also be classified as critical systems. The Board/Partners/Proprietor of the Stockbrokers / Depository Participants shall approve the list of critical systems. To this end, Stockbrokers / Depository Participants should maintain up-to-date inventory of its hardware and systems and the personnel to whom these have been issued, software and information assets (internal and external), details of its network resources, connections to its network and data flows.
2(b)	Has the Stockbrokers / Depository Participants identified / has process to identify cyber risks (threats and vulnerabilities) that it may face, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.
3	**Protection**
3(a)	**Access controls** No person by virtue of rank or position should have any intrinsic right to access, Confidential data, applications, system resources or facilities.

3(b)	**Access control** Any and all access to Stockbrokers / Depository Participants systems, applications, networks, databases etc., have a defined purpose and for a defined period. Stockbrokers / Depository Participants should grant access to IT systems, applications, databases, and networks on a need-to-use basis and based on the principle of least privilege to provide security for both on-and off-premises resources (i.e., zero-trust models). These security models require strict identity verification for each and every resource and device attempting to get access to any information on a private network, regardless of where they are situated, within or outside of a network perimeter. Such access should be for the period when the access is required and should be authorized using multi-factor authentication (MFA). Maker and Checker framework should be implemented in strict manner and enable multi factor authentication (MFA) for all users that connect using online/internet facility and particularly for virtual private networks, webmail and user accounts that access critical systems and applications.
3(c)	Have Stockbrokers / Depository Participants implemented an access policy which addresses strong password controls for users' access to systems, applications, networks, and databases. The policy should include a clause of: 1. Periodic review of accounts of ex-employees. 2. Passwords should not be reused across multiple accounts. 3. List of passwords should not be stored on the system. Illustrative examples for strong password controls are given in Annexure C of SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018
3(d)	All critical systems of the Stockbroker / Depository Participant accessible over the internet should have two-factor security (such as VPNs, Firewall controls etc.)
3(e)	Stockbrokers / Depository Participants should ensure that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes. Such logs should be maintained and stored in a secure location for a time period not less than two (2) years. Stockbrokers / Depository Participants should implement a strong log retention policy as per extant SEBI regulations and required by CERT-In and IT Act 2000.

	Stockbrokers / Depository Participants are advised to audit all logs that are being collected. Stockbrokers / Depository Participants should monitor incidents to identify unusual patterns and behaviors.
3(f)	Stockbrokers / Depository Participants should deploy controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users) to Stockbroker / Depository Participant's critical systems. Such controls and measures should inter-alia include restricting the number of privileged users, periodic review of privileged users' activities, disallow privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, Maker-Checker framework should be implemented for modifying the user's right in internal applications etc.
3(g)	Employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to the Stockbrokers / Depository Participants critical systems, networks, and other computer resources, should be subject to stringent supervision, monitoring, and access restrictions.
3(h)	Stockbrokers / Depository Participants should formulate an Internet access policy to monitor and regulate the use of internet and internet-based services such as social media sites, cloud-based internet storage sites, etc. within the Stockbroker / Depository Participant's critical IT infrastructure.
3(i)	User Management must address deactivation of access of privileges of users who are leaving the organization or whose access privileges have been withdrawn.
4	**Physical Security**
4(a)	Physical access to the critical systems should be restricted to a minimum and only to authorized officials. Physical access of outsourced staff/visitors should be properly supervised by ensuring at the minimum that outsourced staff/visitors are always accompanied by authorized employees.
4(b)	Physical access to the critical systems should be revoked immediately if the same is no longer required.
4(c)	Stockbrokers/ Depository Participants has ensured that the perimeter of the critical equipment's room, if any, are physically secured and monitored by employing physical, human, and procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. where appropriate
5	**Network Security Management**

5(a)	Stockbrokers / Depository Participants has established baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within their IT environment.
5(b)	The LAN and wireless networks should be secured within the Stockbrokers /Depository Participants' premises with proper access controls.
5(c)	For algorithmic trading facilities, adequate measures should be taken to isolate and secure the perimeter and connectivity to the servers running algorithmic trading applications.
5(d)	Stockbrokers / Depository Participants should install network security devices, such as firewalls, proxy servers, intrusion detection and prevention systems (IDS) to protect their IT infrastructure which is exposed to the internet, from security exposures originating from internal and external sources.
5(e)	Adequate controls must be deployed to address virus / malware / ransomware attacks. These controls may include host / network / application-based IDS systems, customized kernels for Linux, anti-virus, and anti-malware software etc.
5(f)	Stockbrokers / Depository Participants should deploy web and email filters on the network. Stockbrokers / Depository Participants should configure these devices to scan for known bad domains, sources, and addresses, block these before receiving and downloading messages. Stockbrokers / Depository Participants should scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.
5(g)	Stockbrokers / Depository Participants should block the malicious domains/IPs after diligently verifying them without impacting the operations. CSIRT-Fin/CERT-In advisories which are published periodically should be referred for latest malicious domains/IPs, C&C DNS and links.
5(h)	Stockbrokers / Depository Participants should restrict execution of "PowerShell" and "wscript" in enterprise environment, if not required. Stockbrokers / Depository Participants should ensure installation and use of the latest version of PowerShell, with enhanced logging enabled, script block logging and transcription enabled. Stockbrokers / Depository Participants should send the associated logs to a centralized log repository for monitoring and analysis.

5(i)	Stockbrokers / Depository Participants should utilize host-based firewall to prevent Remote Procedure Call (RPC) and Server Message Block (SMB) communication among endpoints whenever possible. This limits lateral movement as well as other attack activities.
5(j)	Stockbrokers / Depository Participants should implement the practice of whitelisting of ports based on business usage at Firewall level rather than blacklisting of certain ports. Traffic on all other ports which have not been whitelisted should be blocked by default.
6	**Data security**
6(a)	Critical/sensitive and Personally Identifiable Information (PII) data must be identified, classified, and encrypted in motion and at rest by using strong encryption methods. Illustrative measures in this regard are given in Annexure A and B of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018
6(b)	Stockbrokers / Depository Participants should implement measures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity. It should be ensured that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties. Illustrative measures to ensure security during transportation of data over the internet are given in Annexure B of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018
6(c)	The information security policy should also cover use of devices such as mobile phones, faxes, photocopiers, scanners, etc., within their critical IT infrastructure, that can be used for capturing and transmission of sensitive data. For instance, defining access policies for personnel, and network connectivity for such devices etc.
6(d)	Stockbrokers / Depository Participants should allow only authorized data storage devices within their IT infrastructure through appropriate validation processes.
6(e)	Stockbrokers / Depository Participants should Enforce BYOD (Bring your own device) security policies, like requiring all devices to use a business-grade VPN service and antivirus protection

6(f)	Stockbrokers/ Depository Participants shall deploy detection and alerting tools. Members shall create data leakage prevention (DLP) solutions / processes inclusive of detection, alerting, prevention, containment & response to a data breach/ data leak.
6(g)	Stockbrokers/ Depository Participants shall enforce effective data protection, backup, and recovery measures.
7	**Hardening of Hardware and Software**
7(a)	Whether Member only deploys hardened hardware / software, including replacing default passwords with strong passwords and disabling or removing services identified as unnecessary for the functioning of the system.
7(b)	Whether Open ports on networks and systems which are not in use or that can be potentially used for exploitation of data should be blocked and measures taken to secure them.
8	**Application Security in Customer Facing Applications**
8(a)	Whether over the Internet application like IBTs (Internet Based Trading applications) portal and back-office application, containing sensitive or private information are secured by using security measures. (Illustrative list of measures for ensuring security in such applications is provided in Annexure C of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018
9	**Certification of off-the-shelf products**
9(a)	Stockbrokers / Depository Participants should ensure that off the shelf products being used for core business functionality (such as Back-office applications) should: 1. bear Indian Common criteria certification of Evaluation Assurance Level 4. The Common criteria certification in India is being provided by (STQC) Standardization Testing and Quality Certification (Ministry of Electronics and Information Technology). Or 2. Certified independently on criteria similar to Indian Common Criteria Certificate of Evaluation Assurance Level. Custom developed / in-house software and components need not obtain the certification, but must undergo intensive regression testing, configuration testing etc. The scope of tests should include business logic and security controls.
10	**Patch management**

10(a)	Stockbrokers / Depository Participants should include All operating systems and applications for updating latest patches on a regular basis. Stockbrokers / Depository Participants should establish and ensure that the patch management procedures include the identification, categorization and prioritization of patches and updates. An implementation timeframe for each category of patches should be established to apply them in a timely manner. As an interim measure for zero-day vulnerabilities and where patches are not available, Stockbrokers / Depository Participants can consider virtual patching for protecting systems and networks. This measure hinders cybercriminals from gaining access to any system through vulnerabilities in end-of-support and end-of-life applications and software. Patches should be sourced only from the authorized sites of the OEM.
10(b)	Stockbrokers / Depository Participants should perform rigorous testing of security patches and updates, where possible, before deployment into the production environment to ensure that the application of patches do not impact other systems.
11	**Disposal of data, systems, and storage devices**
11(a)	Stockbrokers / Depository Participants should frame suitable policy for disposal of storage media and systems. The critical data / Information on such devices and systems should be removed by using methods such as crypto shredding / degauss / Physical destruction as applicable.
11(b)	Stockbrokers / Depository Participants should formulate a data-disposal and data-retention policy to identify the value and lifetime of various parcels of data.
12	**Vulnerability Assessment and Penetration Testing (VAPT)**
12(a)	Stockbrokers / Depository Participants shall carry out periodic Vulnerability Assessment and Penetration Tests (VAPT) which inter-alia include critical assets and infrastructure components like Servers, Networking systems, Security devices, load balancers, other IT systems pertaining to the activities done as Stockbrokers / Depository Participants etc., in order to detect security vulnerabilities in the IT environment and in-depth evaluation of the security posture of the system.

12(b)	Stockbrokers / Depository Participants shall conduct VAPT at least once in a financial year. All Stockbrokers / Depository Participants are required to engage only CERT-In empaneled organizations for conducting VAPT. The final report on said VAPT shall be submitted to the Stock Exchanges / Depositories after approval from Technology Committee of respective Stockbrokers / Depository Participants, within 1 month of completion of VAPT activity.
12(c)	In addition, Stockbrokers / Depository Participants shall perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system which is a critical system or part of an existing critical system.
12(d)	In case of vulnerabilities discovered in off-the-shelf products (used for core business) or applications provided by exchange empaneled vendors, Stockbrokers / Depository Participants should report them to the vendors and the exchanges in a timely manner.
12(e)	Any gaps/vulnerabilities detected shall be remedied on immediate basis and compliance of closure of findings identified during VAPT shall be submitted to the Stock Exchanges / Depositories within 3 months post the submission of final VAPT report.
13	**Monitoring and Detection**
13(a)	Stockbrokers / Depository Participants should establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events / alerts and timely detection of unauthorized or malicious activities, unauthorized changes, unauthorised access and unauthorised copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices exposed to the internet should also be monitored for anomalies to identify unusual patterns and behaviors.
13(b)	Further, to ensure high resilience, high availability, and timely detection of attacks on systems and networks exposed to the internet, Stockbrokers / Depository Participants should implement suitable mechanisms to monitor capacity utilization of its critical systems and networks that are exposed to the internet, for example, controls such as firewalls to monitor bandwidth usage.
13(c)	Stockbrokers / Depository Participants should proactively monitor the cyberspace to identify phishing websites w.r.t. to REs/Member domain and report the same to CSIRT-Fin/CERT-In for taking appropriate action.

14	**Response and Recovery**
14(a)	Alerts generated from monitoring and detection systems should be suitably investigated to determine activities that are to be performed to prevent expansion of such incident of cyber-attack or breach, mitigate its effect, and eradicate the incident.
14(b)	The response and recovery plan of the Stockbrokers / Depository Participants should have plans for the timely restoration of systems affected by incidents of cyber-attacks or breaches, for instance, offering alternate services or systems to Customers. Stockbrokers / Depository Participants should have the same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as specified by SEBI for Market Infrastructure Institutions vide SEBI circular CIR/MRD/DMS/17/20 dated June 22, 2012, as amended from time to time
14(c)	The response plan should define responsibilities and actions to be performed by its employees and support / outsourced staff in the event of cyber-attacks or breach of Cyber Security mechanism.
14(d)	Any incident of loss or destruction of data or systems should be thoroughly analyzed
14(e)	And lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes.
14(f)	Stockbrokers / Depository Participants should also conduct suitable periodic drills to test the adequacy and effectiveness of the response and recovery plan. Whether the stockbroker has conducted Periodic DR drills in accordance with Exchange Circular MCX/TECH/726/2022 dated December 16, 2022
15	**Sharing of Information**
15(a)	All Cyber-attacks, threats, cyber-incidents and breaches experienced by Stockbrokers / Depositories Participants shall be reported to Stock Exchanges / Depositories /CERT-IN & SEBI within 6 hours of noticing / detecting such incidents or being brought to notice about such incidents. This information shall be shared to SEBI through the dedicated e-mail id: incident@cert-in.org.in & sbdp-cyberincidents@sebi.gov.in.
15(b)	The incident shall also be reported to Indian Computer Emergency Response team (CERT-In) in accordance with the guidelines / directions issued by CERT-In from time to time.

	Additionally, the Stockbrokers / Depository Participants, whose systems have been identified as “Protected system” by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC.
15(c)	The quarterly reports containing information on cyber-attacks, threats, cyber-incidents and breaches experienced by Stock Brokers / Depository Participants and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities, threats that may be useful for other Stock Brokers / Depository Participants / Exchanges /Depositories and SEBI, shall be submitted to Stock Exchanges / Depositories within 15 days from the quarter ended June, September, December and March of every year.
16	**Training and Education**
16(a)	Stockbrokers / Depository Participants should work on building Cyber Security and basic system hygiene awareness of staff (with a focus on staff from non-technical disciplines).
16(b)	Stockbrokers / Depository Participants should conduct periodic training programs to enhance knowledge of IT / Cyber Security Policy and standards among the employees incorporating up-to-date Cyber Security threat alerts and advisories issued by CERT-In/ CSIRT-Fin that may be referred for assistance in conducting exercises for public awareness. Where possible, this should be extended to outsourced staff, vendors etc. The training programs should be reviewed and updated to ensure that the contents of the program remain current and relevant.
16(c)	Stockbrokers / Depository Participants should Provide training to the employees to avoid clicking on a link in a spear-phishing email, reusing their personal password on a work account, mixing personal with work email and/or work documents, or allowing someone they should not use their corporate device- especially in Work from Home environments.
17	**Systems managed by vendors**
17(a)	Where the systems (IBT, Back office and other Customer facing applications, IT infrastructure, etc.) of a Stock Brokers / Depository Participants are managed by vendors and the Stock Brokers / Depository Participants may not be able to implement some of the aforementioned guidelines directly, the Stock Brokers / Depository Participants should instruct the vendors to adhere to the applicable guidelines in the Cyber Security and Cyber Resilience policy and obtain the necessary self-certifications from them to ensure compliance with the policy guidelines.

18	**SEBI and Exchange Compliances**
18(a)	Auditor to list all applicable implementation of Circulars, Notices, Guidelines, and advisories published by CERT-In/ CSIRT-Fin Advisories, SEBI and Exchanges.
18(b)	Adherence to all such Circulars, Notices, Guidelines, and advisories published
18(c)	Reporting adherences based on prescribed periodicity in point **18(b)** above.
19	**Advisory for Financial Sector Organizations:**
19(a)	Whether compliance of the SEBI circular no. SEBI/HO/MIRSD2/DOR/CIR/P/ 2020/221 dated November 03, 2020, for Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions has been made.
20	**Cyber Security Advisory - Standard Operating Procedure (SOP)**
20(a)	**Cyber Security Advisory** Standard Operating Procedure (SOP) for handling cyber security incidents of intermediaries-as per SEBI directives. The aspects which shall form part of the SOP and whether stockbroker has to complied.
20(b)	Members shall have a well-documented Cyber Security incident handling process document (Standard Operating Procedure - SOP) in place. Such policy shall be approved by Board of the Member (in case of corporate trading member), Partners (in case of partnership firms) or Proprietor (in case of sole proprietorship firm) as the case may be and shall be reviewed annually by the “Internal Technology Committee” as constituted under SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018, for review of Security and Cyber Resilience policy.
20(c)	Members shall examine the Cyber Security incident and classify the Cyber Security incidents into High/ Medium/ Low as per their Cyber Security incident handling process document. The Cyber Security incident handling process document shall define decision on Action/ Response for the Cyber Security incident based on severity.
20(d)	Members shall report the Cyber Security incident to Indian Computer Emergency Response Team (CERT-In).

20(e)	Members shall provide the reference details of the reported Cyber Security incident with CERTI n to the Exchange and SEBI. Members shall also provide details, regarding whether CERT-In team is in touch with the Member for any assistance on the reported Cyber Security incident. If the Cyber Security incident is not reported to CERT-In, members shall submit the reasons for the same to the Exchange and SEBI. Members shall communicate with CERT-In/ Ministry of Home Affairs (MHA)/ Cyber Security Cell of Police for further assistance on the reported Cyber Security incident.
20(f)	Members shall submit details whether Cyber Security incident has been registered as a complaint with law enforcement agencies such as Police or its Cyber Security cell. If yes, details need to be provided to Exchange and SEBI. If no, then the reason for not registering complaint shall also be provided to Exchange and SEBI.
20(g)	The details of the reported Cyber Security incident and submission to various agencies by the Members shall also be submitted to Division Chiefs (in-charge of divisions at the time of submission) of DOS-MIRSD and CISO of SEBI
20(h)	The Designated Officer of the Member (appointed in terms of para 6 of the aforementioned SEBI Circular dated December 03, 2018) shall continue to report any unusual activities and events within 6 hours of receipt of such Information as well as submit the quarterly report on the cyber-attacks & threats within 15 days after the end of the respective quarter in the manner as specified in Exchange circular.
21	**TECHNICAL GLITCH**
21(a)	Member has reported all instances of technical glitches within the prescribed timelines during the audit period in accordance with regulatory guidelines. Member has correctly reported the issues faced and duration of the downtime. Member has implemented all the measures as mentioned in RCAs and has taken necessary steps to prevent the recurrence of such technical glitch.
21(b)	Does the organisation have internal policy to handle technical glitches in accordance with the framework defined in Exchange circular MCX/TECH/726/2022 dated December 16, 2022.

21(c)	Does the policy cover the following: 1. Outline the key systems/departments handling the normal function /operation of the Member and assign responsibilities at business owner and technology owner level. 2. Lay down the processes/steps to be adopted in case of technical glitches along with the timelines and communication with concerned stakeholders including clients. 3. Define the Escalation matrix including reporting of such incident to the Exchange.
21(d)	Whether the stockbroker has reported all instances of technical glitches, issues faced due to glitches and duration of the downtime during the audit period in accordance with Exchange circular MCX/TECH/726/2022 dated December 16, 2022.
21(e)	Whether the stockbroker has implemented measures such as Change Management and Patch Management and the recommended measures as per RCA and taken steps to prevent its recurrence. The System Auditor should review the implemented measures.
21(f)	Whether the stockbroker has maintained adequate Capacity Planning and its review in accordance with Exchange Circular MCX/TECH/726/2022 dated December 16, 2022, for specified member (List of Specified members are provided in Exchange circular MCX/TECH/492/2023 dated July 27, 2023) and for QSB's in accordance with MCX/MEM/358/2023 dated June 01, 2023 (List of QSB's members are provided in Exchange Circular MCX/MEM/154/2023 dated March 06, 2023).
21(g)	Whether the 'Specified Members' have setup ‘automated environments’ in accordance with Exchange Circular MCX/TECH/726/2023 dated December 16, 2022.
21(h)	Whether the stockbroker has obtained the required ISO certifications as recommended by Exchange Circular MCX/TECH/726/2023 dated December 16, 2022
22	**Security of Cloud Services:**
22(a)	Stockbrokers / Depository Participants should check public accessibility of all cloud instances in use. Make sure that no server/bucket is inadvertently leaking data due to inappropriate configurations.
22(b)	Stockbrokers / Depository Participants should ensure proper security of cloud access tokens.

	The tokens should not be exposed publicly in website source code, any configuration files etc.
22(c)	Stockbrokers / Depository Participants should implement appropriate security measures for testing, staging and backup environments hosted on cloud. Ensure that the production environment is kept properly segregated from these. Disable/remove older or testing environments if their usage is no longer required.
22(d)	Stockbrokers / Depository Participants should consider employing hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments.
22(e)	Governance, Risk and Compliance (GRC) Ensure alignment with Governance, Risk, and Compliance (GRC) standards within cloud computing operations and practices. Refer principle 1 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023
22(f)	Selection of Cloud Service Providers Ensure compliance with established guidelines and protocols in the selection and engagement of cloud service providers. Refer principle 2 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023
22(g)	Data Ownership and Data Localization Ensure compliance with data ownership and localization requirements as mandated by relevant regulations and policies within cloud operations. Refer principle 3 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023
22(h)	Responsibility of the Regulated Entity Ensure that the Regulated Entity assumes responsibility for maintaining compliance with all relevant cloud computing regulations and standards. Refer principle 4 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023
22(i)	Due Diligence by the Regulated Entity Ensure that the Regulated Entity conducts thorough due diligence when assessing cloud service providers and their compliance with regulatory requirements. Refer principle 5 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023

22(j)	Security Controls: Implement and maintain robust security controls to safeguard data and systems in compliance with cloud computing regulations and standards. Refer principle 6 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023
22(k)	Contractual and Regulatory Obligations: Ensure that contractual agreements with cloud service providers align with regulatory obligations to maintain compliance within cloud operations. Refer principle 7 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023
22(l)	BCP, Disaster Recovery & Cyber Resilience Integrate Business Continuity Planning (BCP), Disaster Recovery, and Cyber Resilience measures into cloud operations to ensure compliance with regulatory requirements. Refer principle 8 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023
22(m)	Vendor Lock-In and Concentration Risk Management Implement strategies to manage vendor lock-in and concentration risks effectively in cloud operations to maintain compliance with regulatory standards. Refer principle 9 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023
23	**Concentration Risk on Outsourced Agencies:**
23(a)	Stockbrokers / Depository Participants should take into account concentration risk (Single third-party vendors are providing services to multiple Stockbrokers / Depository Participants) while outsourcing multiple critical services to the same vendor.

Annexure 5

Cyber Incident Reporting

Incident Reporting Form		
1. Letter / Report Subject -		
Name of the Member / Depository Participant - Name of the Stock Exchange / Depository - Member ID / DP ID -		
2. Reporting Periodicity Year-		
☐ Quarter 1 (Apr-Jun) ☐ Quarter 2 (Jul-Sep)	☐ Quarter 3 (Oct-Dec) ☐ Quarter 4 (Jan-Mar)	
3. Designated Officer (Reporting Officer details) -		
Name:	Organization:	Title:
Phone / Fax No:	Mobile:	Email:
Address:		
Cyber-attack / breach observed in Quarter: (If yes, please fill Annexure I) (If no, please submit the NIL report)		
Date & Time	Brief information on the Cyber-attack / breached observed	
Annexure I		
1. Physical location of affected computer / network and name of ISP -		

2. Date and time incident occurred -
Date: Time:
3. Information of affected system -

IP Address:	Computer / Host Name:	Operating System (incl. Ver. / release No.):	Last Patched/ Updated:	Hardware Vendor/ Model:

4. Type of incident -

☐ Phishing ☐ Network scanning /Probing Break-in/Root Compromise ☐ Virus/Malicious Code ☐ Website Defacement ☐ System Misuse	☐ Spam ☐ Bot/Botnet ☐ Email Spoofing ☐ Denial of Service(DoS) ☐ Distributed Denial of Service(DDoS) ☐ User Account Compromise	☐ Website Intrusion ☐ Social Engineering ☐ Technical Vulnerability ☐ IP Spoofing ☐ Ransomware ☐ Other____

5. Description of incident -
6. Unusual behavior/symptoms (Tick the symptoms) -

☐ System crashes ☐ New user accounts/ Accounting discrepancies ☐ Failed or successful social engineering attempts ☐ Unexplained, poor system performance ☐ Unaccounted for changes in the DNS tables, router rules, or firewall rules ☐ Unexplained elevation or use of privileges Operation of a program or sniffer device to capture network traffic; ☐ An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user ☐ A system alarm or similar indication from an intrusion detection tool ☐ Altered home pages, which are usually the intentional target for visibility, or other pages on the Web server	☐ Anomalies ☐ Suspicious probes ☐ Suspicious browsing New files ☐ Changes in file lengths or dates ☐ Attempts to write to system ☐ Data modification or deletion ☐ Denial of service ☐ Door knob rattling ☐ Unusual time of usage ☐ Unusual usage patterns ☐ Unusual log file entries ☐ Presence of new setuid or setgid files Changes in system directories and files ☐ Presence of cracking utilities ☐ Activity during non-working hours or holidays ☐ Other (Please specify)
7. Details of unusual behavior/symptoms -	

8. Has this problem been experienced earlier? If yes, details -			
9. Agencies notified -			
Law Enforcement	Private Agency	Affected Product Vendor	Other _____
10. IP Address of apparent or suspected source -			
Source IP address:		Other information available:	
11. How many host(s) are affected -			
1 to 10	10 to 100	More than 100	
12. Details of actions taken for mitigation and any preventive measure applied -			

Annexure 6

VAPT report format

VAPT Report Summary				
Name of Entity				
Name of Trading Member				
Contact person Details (Name, Mobile number & Email ID) of Trading Member (Preferably CISO's)				
VAPT Completion Date “(DD-MM-YYYY)”				
Date of approval of VAPT report by Technology Committee of Trading Member “(DD-MM-YYYY)”				
Name of the Auditor				
Name of the Audit Firm				
Audit Firm Landline No.				
Auditor Mobile No.				
Auditor / Audit Firm Email ID				
CERT-In empanelment validity expiry Date (DD-MM-YYYY)				
	Critical	**High**	**Medium**	**Low**
No of identified vulnerabilities ((A) + (B))				
(A) No of closed vulnerabilities				
(B) No of open vulnerabilities				
Reason for non-closure: Mention for Critical, Medium and Low separately				
Remarks				
Contact Details of Entity (Preferably CISO's)				
Submitted by:	Date:			

Annexure 7

Action Taken Report / Compliance Report on the non-conformities / vulnerabilities identified during the VAPT conducted during the FY _____.

Particulars	**Critical**	**High**	**Medium**	**Low**
No. of Open Vulnerabilities as reported in VAPT report submitted to the Exchange				
Current Status				

Explanation / Reason for non-closure

(To be filled in case of open vulnerabilities mentioned in current status)

Details of such open Non Conformities / Vulnerabilities*	**Explanation / Reason for Non Closure**

***Open vulnerabilities shall attract appropriate penalty by the Exchange depending on the criticality / such other factors**

Auditor Name:		Auth. Signatory Name:	
Name of Auditor entity:		Trading Member (TM) Name & TM ID:	
Sign:		Sign:	

(To be signed by CERT-In empaneled auditor as appointed by the Member and by authorized official of the Member)

Annexure 8

Technical Glitch – List of Specified Members

Sl. No.	Trading Member Name
1	5paisa Capital Limited
2	Acumen Capital Market (India) Limited
3	Alice Blue Financial Services Private Limited
4	Anand Rathi Share and Stock Brokers Limited
5	Angel One Limited
6	Axis Securities Limited
7	Bonanza Commodity Brokers Private Limited / Bonanza Portfolio Limited
8	Choice Equity Broking Private Limited
9	Dhani Stocks Limited
10	Nuvama Wealth and Investment Limited
11	Finvasia Securities Private Limited
12	Fyers Securities Private Limited
13	Geojit Financial Services Limited
14	Goodwill Wealth Management Private Limited
15	HDFC Securities Limited
16	ICICI Securities Limited
17	IIFL Securities Limited
18	Kotak Securities Limited
19	Moneylicious Securities Private Limited
20	Motilal Oswal Financial Services Limited
21	Nextbillion Technology Private Limited
22	Nirmal Bang Securities Private Limited
23	NJ India Invest Private Limited
24	Paytm Money Limited
25	Profitmart Securities Private Limited
26	Reliance Securities Limited
27	Religare Broking Limited
28	RKSV Securities India Private Limited
29	SBICAP Securities Limited
30	Sharekhan Limited
31	SMC Global Securities Limited
32	Swastika Investmart Limited

Sl. No.	Trading Member Name
33	Ventura Securities Limited
34	Zebu Share and Wealth Managements Private Limited
35	Zerodha Broking Limited / Zerodha Commodities Private Limited
36.	Globe Capital Market Limited
37.	Jainam Broking Limited

Annexure 9

"ANNEXURE B" INTIMATION & SUBMISSION OF TECHNICAL GLITCH		
	HEADERS	DETAILS
1. Intimation of Incident (T-day, within 1 Hour of the Incident)	1. Letter / Report Subject -	
	Name of the Member --	
	Member Code -	
	2. Designated Officer (Reporting Officer details)	Name:
		Mobile:
		Email ID:
	3. Date & Time of Incident	
	4. Exchanges on which Technical Glitch was encountered (NSE, BSE, MCX, NCDEX, MSEI)	
	5. Intimation to clients about the Technical Glitch. (Please attach screenshots of communications to clients)	
	6. Network Connectivity Issues / Hardware Issues / Software Issues / Human Error / Other (Please Specify (if more than one, please separate with commas))	
	7. Additional Details about the Technical Glitch, if Any.	
2. Preliminary Incident Report (T+1 day)	1. Date & Time of Incident & Incident duration (in Minutes)	
	2. Incident Description	
	3. Immediate action taken (provide brief details)	
	4. Business Impact i) Number of Clients Impacted ii) Any other impact	
	5. Were alternate trading channles available for clients (list all the alternate channels)	

	i) Was there a spike in traffic on the alternate channels available to clients? If yes, provide details.	
	6. Was the issue caused or encountered by a thirdparty vendor or service provider? i) Name of the third-party vendor or service provider and a bief description of the issue. ii) Do you have a back-up vendor for the said services	
	7. Was the issue encountered on the Exchange provided environment? If Yes, kindly provide details of initimation and communication sent to the Exchange.	
	8. Did you move operations to the Disaster Recover (DR) site? If, Yes, what was the Recovery Time?	
3. RCA of Technical Glitch Incident (T + 14 days)	1. Date & Time of Incident & Recovery & Incident duration (in Minutes)	
	2. Incident Description & chronology of events (Please provide brief details)	
	3. Business Impact: Please provide details on the points below: i) Number of clients impacted ii) Number of client orders impacted iii) Any P&L impact iv) Any other impact on Business	
	4. Details of Client Complaints Received (Please provide details of claims of impacted clients) i) Number of Complaints Received ii) Number of Complaints Settled iii) Number of pending complaints iv) Total amount claimed by complainants	
	5. Root Cause Summary (Pl attach the detailed Report separately)	

	6. If the issue was caused or encountered by a thirdparty vendor or service provider, Please provide the below details: **i)** What services are being provided by the thirdparty vendor or service provider? **ii)** Time taken (in Minutes) by third-party vendor or service provider to resolve the issue.	
	7. Has a similar issue been encountered prior to the submission of this RCA Report?	
	8. Details of long-term preventive action (please provide all action points for long-term preventive action with the date from which they will be implemented) (please use additional sheets if necessary)	
	9. Provide a detailed Architecture Diagram of the System.	

Annexure 10

AI and ML

Annexure 1 - Form to report on AI and ML technologies – To be submitted quarterly		
Intimation to Stock Exchange / Depository for the use of the AI and ML application and systems.		
SNo.	**Head**	**Value**
1	Entity SEBI registration number	
2	Registered entity category	
3	Entity name	
4	Entity PAN no.	
5	Application / System name	
6	Date from when the Application / System was used	
7	Type of area where AI or ML is used	<order execution / Advisory services / KYC / AML / Surveillance / compliance/others (please specify in 256 characters)>
7.a	Does the system involve order initiation, routing and execution?	<Yes / NO>
7.b	Does the system fall under discretionary investment or Portfolio management activities?	<Yes / NO>
7.c	Does the system disseminate investment or trading advice or strategies?	<Yes / NO>
7.d	Is the application/system used in area of Cyber Security to detect attacks	<Yes / NO>
7.e	What claims have been made regarding AI and ML Application / System – if any?	<free text field>
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 to circular of SEBI that mandate cyber security control requirements	<free text field>
11	Is the AI / ML system included in the system audit, if applicable?	<Yes / NO / NA>
12	Describe the application / system and how it uses AI / ML as portrayed in the product offering	<Yes / NO>
13	What safeguards are in place to prevent abnormal behavior of the AI or ML application / System	<Yes / NO>

Annexure 11

Format for Submission of Details of Cloud Deployments

The REs shall provide details of their cloud deployment in the following format-

A. Entity Name:

B. Entity Type: (For example stock exchange, depository, mutual fund, etc.) C. Whether Utilizing Cloud Services? Yes/ No

For Each Cloud application/ service/ system, please provide a response to the following:

SN	Details Required	***Entity Response***
1	Name of the Application/ Service/ System	
2	The type of deployment model utilized (public cloud, community cloud, etc.)	
3	The type of service model utilized (For example IaaS, PaaS, etc.)	
4	Name of the Cloud Service Provider (CSP)	
5	Country of incorporation/ registration of CSP	
	Name of the Managed Service Provider (MSP) / System Integrator (SI) [wherever applicable]	
6	Country of incorporation/ registration of MSP/ SI	
7	Whether the application/ service/ system is a critical or core application/ service/ system?	
8	Details of Data hosted/ stored in cloud	
9	Whether data is stored within the legal boundaries of India?	

Annexure 12

Software as a Service SaaS

<<Member Name>>
<<Address>>
<<Email Address>>
<<Information Security Contact Person>>

"Compliance of the SEBI circular for Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions"

This communication is a pursuant to Circular - **MCX/TECH/309/2021** dated May 24, 2021

Under guidance received from SEBI as per circular -

SEBI/HO/MIRSD2/DOR/CIR/P/2020/221 & subsequent Amber advisory from CERT-IN – 201155100308.

<<**Member Name**>> would like to confirm that specified confidential data and data types (as specified in the CERT-IN advisory) are **hosted / not hosted** on with SaaS provider/ <<**Member Name**>> use or does not use any SaaS based GRC solutions. **Half-yearly report** for the period **July XXXX to December XXXX OR January XXXX to June XXXX.**

Kindly provide your responses in the below format.

CSP Name	Nature of service consumed	Environment usage (Including nature of data exchanged)	Geo-Location for hosting	Gaps against Circular	Deadline to close the Gaps

*CSP – Cloud Service Providers

Annexure 13

Advisory for SEBI Regulated Entities (REs) regarding Cybersecurity best practices

Compliance Report

(To be printed on company letter-head)

Member ID:
Member Name:
Contact Person name:
Contact Person Mobile no:

I/We hereby confirm on compliance to the Advisory for SEBI Regulated Entities (REs) regarding Cybersecurity best practices recommended by CSIRT-Fin through SEBI Circular No: SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/032, Dated February 22, 2023.

Sr.No.	Requirement	Compliant/Non-Compliant/Not Applicable	Remark (To justify why points are Not Applicable)
1	**Roles and Responsibilities of Chief Information Security Officer (CISO)/Designated Officer:** REs/Member are advised to define roles and responsibilities of Chief Information Security Officer (CISO) and other senior personnel. Reporting and compliance requirements shall be clearly specified in the security policy.		
2	**Measures against Phishing attacks/ websites:** i. The REs/Member need to proactively monitor the cyberspace to identify phishing websites w.r.t. to REs/Member domain and report the same to CSIRT-Fin/CERT-In for taking appropriate action.		
	ii. Majority of the infections are primarily introduced via phishing emails, malicious adverts on websites, and third-party apps and programs. Hence, thoughtfully designed security awareness campaigns that stress the avoidance of clicking on links and attachments in email, can establish an essential pillar of defence. Additionally, the advisories issued by CERT-In/ CSIRT-Fin may be referred for assistance in conducting exercises for public awareness.		

3	**Patch Management and Vulnerability Assessment and Penetration Testing (VAPT):** i. All operating systems and applications should be updated with the latest patches on a regular basis. As an interim measure for zero-day vulnerabilities and where patches are not available, virtual patching can be considered for protecting systems and networks. This measure hinders cybercriminals from gaining access to any system through vulnerabilities in end-of-support and end-of-life applications and software. Patches should be sourced only from the authorized sites of the OEM.		
	ii. Security audit / Vulnerability Assessment and Penetration Testing (VAPT) of the application should be conducted at regular basis and in accordance with the Cyber Security and Cyber Resilience circulars of SEBI issued from time to time. The observation/ gaps of VAPT/Security Audit should be resolved as per the timelines prescribed by SEBI.		
4	**Measures for Data Protection and Data breach:** i. REs/Member are advised to prepare detailed incident response plan.		
	ii. Enforce effective data protection, backup, and recovery measures.		
	iii. Encryption of the data at rest should be implemented to prevent the attacker from accessing the unencrypted data.		
	iv. Identify and classify sensitive and Personally Identifiable Information (PII) data and apply measures for encrypting such data in transit and at rest.		
	v. Deploy data leakage prevention (DLP) solutions / processes.		
5	**Log retention:** Strong log retention policy should be implemented as per extant SEBI regulations and required by CERT-In and IT Act 2000. REs/Member are advised to audit that all logs are being collected. Monitoring of all logs of events and incidents to identify unusual patterns and behaviours should be done. Refer SEBI circular CIR/MIRSD/24/2011 dated December 15, 2011.		
6	**Password Policy/ Authentication Mechanisms:** i. Strong password policy should be implemented. The policy should include a clause of periodic review of accounts of ex-employees Passwords should not be reused across		

	multiple accounts or list of passwords should not be stored on the system.		
	ii. Enable multi factor authentication (MFA) for all users that connect using online / internet facility and also particularly for virtual private networks, webmail and accounts that access critical systems. iii. Maker and Checker framework should be implemented in strict manner and MFA should be enabled for all user accounts, especially for user accounts accessing critical applications.		
7	**Privilege Management:** i. Maker-Checker framework should be implemented for modifying the user's right in internal applications. ii. For mitigating the insider threat problem, 'least privilege' approach to provide security for both on-and off-premises resources (i.e., zero-trust models) should be implemented. Zero Trust is rooted in the principle of "trust nothing, verify everything." This security model requires strict identity verification for each and every resource and device attempting to get access to any information on a private network, regardless of where they are situated, within or outside of a network perimeter.		
8	**Cybersecurity Controls:** i. Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses, block these before receiving and downloading messages. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.		
	ii. Block the malicious domains/IPs after diligently verifying them without impacting the operations. CSIRT-Fin/CERT-In advisories which are published periodically should be referred for latest malicious domains/IPs, C&C DNS and links.		
	iii. Restrict execution of "powershell" and "wscript" in enterprise environment, if not required. Ensure installation and use of the latest version of PowerShell, with enhanced logging enabled, script block logging and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis.		
	iv. Utilize host based firewall to prevent Remote Procedure Call (RPC) and Server Message Block (SMB)		

	communication among endpoints whenever possible. This limits lateral movement as well as other attack activities.		
	v. Practice of whitelisting of ports based on business usage at Firewall level should be implemented rather than blacklisting of certain ports. Traffic on all other ports which have not been whitelisted should be blocked by default.		
9	**Security of Cloud Services:** i. Check public accessibility of all cloud instances in use. Make sure that no server/bucket is inadvertently leaking data due to inappropriate configurations. ii. Ensure proper security of cloud access tokens. The tokens should not be exposed publicly in website source code, any configuration files etc. iii. Implement appropriate security measures for testing, staging and backup environments hosted on cloud. Ensure that production environment is kept properly segregated from these. Disable/remove older or testing environments if their usage is no longer required. iv. Consider employing hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments.		
10	**Implementation of CERT-In/ CSIRT-Fin Advisories:** The advisories issued by CERT-In should be implemented in letter and spirit by the regulated entities. Additionally, the advisories should be implemented promptly as and when received.		
11	**Concentration Risk on Outsourced Agencies:** i. It has been observed that single third party vendors are providing services to multiple Res/Members, which creates concentration risk. Here, such third parties though being small non-financial organizations, if any cyberattack, happens at such organizations, the same could have systemic implication due to high concentration risk. ii. Thus, there is a need for identification of such organizations and prescribing specific cyber security controls, including audit of their systems and protocols from independent auditors, to mitigate such concentration risk. iii. Further, REs/Member also need to take into account this concentration risk while outsourcing multiple critical services to the same vendor.		
12	**Audit and ISO Certification:**		

	i. SEBI's instructions on external audit of REs/Member by independent auditors empanelled by CERT-In should be complied with in letter and spirit.		
	ii. The REs/Member are also advised to go for ISO certification as the same provides a reasonable assurance on the preparedness of the RE/Member with respect to cybersecurity.		
	iii. Due diligence with respect to audit process and tools used for such audit needs to be undertaken to ensure competence and effectiveness of audits		

I/We certify that all the statements are true and correct to the best of our knowledge.

Place:
Date:

Signature of the CISO/CIO/CTO/Head of IT & Stamp

Glossary

Abbreviation	Meaning
AI & ML	Artificial Intelligence (AI) and Machine Learning (ML)
ASP	Application Service Provider
ATF	Algorithmic Trading Facility
BCP / DR	Business Continuity Plan / Disaster Recovery
CISA	Certified Information System Auditors from ISACA
CISM	Certified Information Securities Manager from ISACA
CISSP	Certified Information Systems Security Professional
CTCL	Computer to Computer Link
DISA	Diploma in Information System Audit from ICAI
FIX	Financial Exchange Information
FMC	Forward Market Commission
IBT	Internet Based Trading
ICAI	Institute of Chartered Accountants of India
ISV	Independent Software Vendor
MCX	Multi Commodity Exchange of India Limited
RMS	Risk Management System
SEBI	Securities Exchange Board of India
TOR	Terms of Reference
WT / STWT	Wireless Trading
SAR	System Audit Report
CSCR	Cyber Security & Cyber Resilience Audit Report
CERT-In	Computer Emergency Response team
NCIIPC	National Critical Information Infrastructure Protection Centre
VAPT	Vulnerability Assessment and Penetration Testing
RCA	Rout Cause Analysis
LAMA	Logging and Monitoring Mechanism
SaaS	Software as a Service
IRRA	Investor Risk Reduction Access