भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

CIRCULAR for Market Infrastructure Institutions on common Information Technology related provisions

1. ANNUAL SYSTEM AUDIT 3

1.1. System and Network Audit of Market Infrastructure Institutions 3

1.2. Advisory on System and Network Audit of MIIs 4

2. BUSINESS CONTINUITY PLAN AND DISASTER RECOVERY 6

2.1. Guidelines for Business Continuity Plan (BCP) and Disaster Recovery (DR) of Market Infrastructure Institutions (MIIs) 6

2.2. Business Continuity Plan (BCP) and Disaster Recovery (DR) framework – Limited Purpose Clearing Corporation (LPCC) 10

2.3. Standard Operating Procedure for handling of technical glitches by Market Infrastructure Institutions (MIIs) and payment of "Financial Disincentives" thereof 10

2.4. Advisory for reporting of technical glitches 11

2.5. Measures to strengthen tracking and reporting of delay in pay-in/pay-out for rolling settlement 12

2.6. Advisory on Security Patch Management Policy 14

All the MIIs are advised to ensure the following: 14

2.7. Standard Operating Procedure for handling of Stock Exchange Outage and extension of trading hours thereof 14

2.8. Testing Framework for the Information Technology (IT) Systems of the Market Infrastructure Institutions (MIIs) 19

2.9. Business Continuity for Clearing Corporations through Software as a Service (SaaS) Model (except Commodity Derivatives Exchanges and Clearing Corporations) 21

Outline of SaaS model for RMS: 21

2.10. Business Continuity for Interoperable Segments of Stock Exchanges 24

2.11. Advisory on Business Continuity and Disaster Recovery 25

3. CYBER SECURITY AND CYBER RESILIENCE 26

3.1. Cyber Security and Cyber Resilience framework – Limited Purpose Clearing Corporation (LPCC) 26

3.2. Strengthening Resiliency of Websites of Stock Exchanges, Clearing Corporations and Depositories (MIIs) 26

3.3. Bolstering Cyber Resiliency 27
3.4. Cyber Security and Cyber Resilience framework of MIIs 27
3.5. Reporting for Artificial Intelligence (AI) and Machine Learning (ML) applications and systems offered and used by Market Infrastructure Institutions (MIIs) 31
3.6. Standard Operating Procedure for reporting of Cyber Security breaches, incidents and deficiencies and for imposition of "Financial Disincentive" on Market Infrastructure Institutions (MIIs) 32
3.7. Advisory on Cyber Audit and VAPT 36
3.8. Advisory on Cyber security and Cyber resilience 36
4. CAPACITY PLANNING 38
4.1. Capacity planning and Real Time Performance Monitoring framework of Market Infrastructure Institutions(MIIs), ... 38
5. ADVISORIES RELATED TO TECHNOLOGY 41
5.1. Advisory on Technology related Investments and Planning by Market Infrastructure Institutions (MIIs) 41
5.2. Advisory on automation/review of operational processes involving IT systems of Market Infrastructure Institutions (MIIs) 41
5.3. Process for freezing/un-freezing of accounts/holdings pursuant to issuance of orders of SEBI/ Securities Appellate Tribunal(SAT)/ Supreme Court of India/ other courts 42
5.4. Segregation of IT Infrastructure and activities between Stock Exchanges and Clearing Corporations 44
6. REFERENCE: List of Circulars 45
Annexure I 46
Annexure II 51
Annexure III 58
Annexure IV 59
Annexure IVA 62
Annexure V 68
Annexure VI 69
Annexure VII 71
Annexure VIII 74
Annexure IX – Systems deemed to be based on AI and ML technology 78
Annexure X - Form to report on AI and ML technologies – to be submitted quarterly 79

1. ANNUAL SYSTEM AUDIT

1.1. System and Network Audit of Market Infrastructure Institutions [1]

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

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

1.1.3. The Systems and Network Audit Report including compliance with SEBI circulars/ guidelines and exceptional observation format along with compliance status of previous year observations and comments of their Technology Committee on report shall be communicated to SEBI within three months from the end of audit period. Additional comment(s) of the Governing Board (if any) on the report, if not received within three months, shall be submitted at the earliest to SEBI, not later than seven days, after the next meeting of the Governing Board post completion of audit. A standardized format for System and Network Audit report for MIIs has been provided in Annexure IVA[2].

1.1.4. Further, along with the audit report, MIIs are required to submit a Joint declaration from the Managing Director(MD)/Chief Executive Officer(CEO) and Chief Technology Officer (CTO) certifying a) the security and integrity of their IT Systems b) correctness and completeness of data provided to the Auditor c) entire network architecture, connectivity (including co-lo facility) and its linkage to the trading infrastructure are in conformity with SEBI's regulatory framework to provide fair equitable, transparent and non-discriminatory treatment to all the market participants d) internal review of Critical Systems as defined in Clause

[1] Circular No. SEBI/HO/MRD1/MRD1_DTCS/P/CIR/2022/58 dated May 02, 2022
[2] Circular No. SEBI/HO/MRD/TPD/CIR/P/2025/50 dated April 04,2025

2.1 of this Circular for MIIs was carried out during the Audit period, including the Failure Modes and Effects Analysis (FMEA).

1.2. **Advisory on System and Network Audit of MIIs**

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

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

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

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

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

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

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

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

1.2.8. System and network audit report shall include the point-wise compliance of areas emanating from relevant SEBI circulars/directions/advices along with any accompanying evidence.

1.2.9. Auditor shall certify that entire network architecture, connectivity (including co-lo facility) and its linkage to the trading infrastructure are in conformity with SEBI's regulatory framework to provide fair equitable, transparent and non-discriminatory treatment to all the market participants.

1.2.10. Evidence verified/checked by auditor to ascertain the compliance of particular control shall be in line with the intent/requirement of the said control mentioned in the SEBI circular pertaining to system and network audit.

1.2.11. All MIIs shall strictly comply with the said advisory, bring the same to the notice of the concerned system and network auditors and provide compliance of the aforesaid advisory along with their system and network audit report.

2. BUSINESS CONTINUITY PLAN AND DISASTER RECOVERY

2.1. Guidelines for Business Continuity Plan (BCP) and Disaster Recovery (DR) of Market Infrastructure Institutions (MIIs)[3]

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

2.1.1.1. Stock Exchanges and Clearing Corporations (which, along with Depositories, are collectively referred as Market Infrastructure Institutions – MIIs) shall have in place BCP and DRS so as to maintain data and transaction integrity.

2.1.1.2. For Stock Exchanges: Apart from DRS, all Stock Exchanges shall also have a Near Site (NS) to ensure near zero data loss.

For Clearing Corporations and Depositories: Apart from DRS, all Clearing Corporations and Depositories shall also have a Near Site (NS) to ensure zero data loss

2.1.1.3. The DRS should preferably be set up in different seismic zones and in case due to certain reasons such as operational constraints, change of seismic zones, etc., minimum distance of 500 kilometer shall be ensured between Primary Data Centre (PDC) and DRS so that both DRS and PDC are not affected by the same disaster.

2.1.1.4. The manpower deployed at DRS shall have the same expertise as available at PDC in terms of knowledge/ awareness of various technological and procedural systems and processes relating to all operations such that DRS can function at short notice, independently. MIIs shall have sufficient number of trained staff at their DRS so as to have the capability of running live operations from DRS without involving staff of the PDC.

2.1.1.5. All MIIs shall constitute an Incident and Response team (IRT)/ Crisis Management Team (CMT), which shall be chaired by the Managing Director (MD) of the MII or by the Chief Technology Officer (CTO), in case of non-availability of MD. IRT/ CMT shall be responsible for the actual declaration of disaster, invoking the BCP and shifting of operations from PDC to DRS whenever required. Details of roles, responsibilities and actions to be performed by employees, IRT/ CMT and support/outsourced staff in the event of any Disaster shall be defined and documented by the MII as part of BCP-DR Policy Document.

[3] Circular No. SEBI/HO/MRD1/DTCS/CIR/P/2021/33 dated March 22, 2021 and SEBI Circular SEBI/HO/MRD/TPD-1/P/CIR/2024/119 dated September 12, 2024

2.1.1.6. The Standing Committee on Technology (SCOT) of the MIIs shall review the implementation of BCP-DR policy approved by the Governing board of the MII on a quarterly basis.

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

2.1.2. **Configuration of DRS/NS with PDC**

2.1.2.1. Hardware, system software, application environment, network and security devices and associated application environments of DRS / NS and PDC shall have one to one correspondence between them at any point of time to ensure seamless and rapid recovery in case of a disaster (defined below). There shall be no exception unless approved by SEBI as per the recommendation of the Technology Advisory Committee (TAC) of SEBI.

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

2.1.2.3. In the event of disruption of any one or more of the 'Critical Systems' (as defined below), the MII shall, within 30 minutes of the incident, declare that incident as 'Disaster' and take measures to restore operations including from DRS within 45 minutes of the declaration of 'Disaster'. Accordingly, the Recovery Time Objective(RTO)- the maximum time taken to restore operations of 'Critical Systems' from DRS after declaration of Disaster- shall be 45 minutes. 'Critical Systems' for the above purpose for an Exchange/ Clearing Corporation shall include Trading, Risk Management, Collateral Management, Clearing and Settlement and Index computation. 'Critical Systems' for a Depository shall include systems supporting settlement process and inter-depository transfer system. Further, MIIs may include additional systems as critical systems as per defined policy in this regard.

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

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

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

2.1.2.6. Any updates pertaining to critical systems and application releases made at the PDC should be reflected at DRS/ NS before beginning of next day with head room flexibility without compromising any of the performance metrics. For reflecting other updates at DRS/NS, timeline specified in Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (SEBI Circular Number SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024) shall be complied with (timeline specified for DRS to be considered for NS in case timeline is not specified for NS in CSCRF). For exceptions, MIIs shall consult SCOT and seek its guidance for relaxation in case of unavoidable reasons.

2.1.2.7. Replication architecture, bandwidth and load consideration between the DRS / NS and PDC should be within stipulated RTO and ensure high availability, right sizing, and no single point of failure.

2.1.2.8. For Stock Exchanges: Synchronous replication or appropriate replication between PDC and NS shall be implemented to ensure near zero data loss. Asynchronous replication may be implemented between PDC and DRS and between NS and DRS.

For Clearing Corporations and Depositories: Synchronous replication between PDC and NS shall be implemented to ensure zero data loss. Asynchronous replication may be implemented between PDC and DRS and between NS and DRS.

2.1.2.9. Adequate resources (with appropriate training and experience) should be available at all times to handle operations at PDC, NS or DRS, as the case may be, on a regular basis as well as during disasters.

2.1.3. **DR drills/ Testing**

2.1.3.1. DR drills should be conducted on a quarterly basis. In case of Exchanges and Clearing Corporations, these drills should be closer to real life scenario (trading days) with minimal notice to DRS staff involved.

2.1.3.2. During the drills, the staff based at PDC should not be involved in supporting operations in any manner.

2.1.3.3. The drill should include running all operations from DRS for at least 1 full trading day.

2.1.3.4. Before DR drills, the timing diagrams including details of all DR activities with planned timelines and clearly identifying resources at both ends (DRS as well as PDC) should be in place.

2.1.3.5. The results and observations of these drills along with comments of the Standing Committee on Technology (SCOT) of MII shall be forwarded to SEBI within a month of the drill. Additional comment(s) of the Governing Board of MII, if any, shall also be submitted to SEBI at the earliest, not later than seven days, after the next meeting of Governing Board post DR drill.

2.1.3.6. The System Auditor while covering the BCP – DR as a part of mandated annual System Audit should check the preparedness of the MII to shift its operations from PDC to DRS unannounced and also comment on documented results and observations of DR drills.

2.1.3.7. 'Live' trading sessions from DR site shall be scheduled for at least two consecutive days in every six months. Such live trading sessions from the DRS shall be organized on normal working days (i.e. not on weekends / trading holidays). The MII shall ensure that staff members working at DRS have the abilities and skills to run live trading session independent of the PDC staff. Further, DR drills as envisaged in paragraph 2.1.3.1 may not be conducted in the quarter when half yearly live trading sessions as envisaged in this paragraph is being conducted.

2.1.3.8. MII shall include a scenario of intraday shifting from PDC to DRS during the mock trading sessions in order to demonstrate its preparedness to meet RTO/RPO as stipulated above.

2.1.3.9. MII should undertake and document Root Cause Analysis (RCA) of their technical/ system related problems in order to identify the causes and to prevent reoccurrence of similar problems.

2.1.4. **BCP – DR Policy Document**

2.1.4.1. MIIs shall put in place a comprehensive BCP-DR policy document outlining the following:

2.1.4.1.1. Broad scenarios that would be defined as a Disaster for an MII (in addition to definition provided in para 2.1.2.3 of the circular).

2.1.4.1.2. Standard Operating Procedure to be followed in the event of Disaster.

2.1.4.1.3. Escalation hierarchy within the MII to handle the Disaster.

2.1.4.1.4. Clear and comprehensive Communication Protocols and procedures for both internal and external communications from the time of incident till resumption of operations of the MII.

2.1.4.1.5. Documentation policy on record keeping pertaining to DR drills.

2.1.4.1.6. Scenarios demonstrating the preparedness of MIIs to handle issues in Critical Systems that may arise as a result of Disaster.

2.1.4.1.7. Preparedness of Depositories to handle any issue which may arise due to trading halts in Stock Exchanges.

2.1.4.1.8. Framework to constantly monitor health and performance of Critical Systems in normal course of business.

2.1.4.2. The BCP-DR policy document of MII should be approved by Governing Board of the MIIs after being vetted by SCOT. The BCP-DR policy document should be periodically reviewed at least once in a year and after every occurrence of disaster.

2.1.4.3. In case an MII desires to lease its premise at the DRS to other entities including to its subsidiaries or entities in which it has stake, the MII should ensure that such arrangements do not compromise confidentiality, integrity, availability, targeted performance and service levels of the MII's systems at the DRS. The right of first use of all the resources at DRS including network resources should be with the MII. Further, MII should deploy necessary access controls to restrict access (including physical access) of such entities to its critical systems and networks.

2.1.5. MIIs should ensure that clauses 2.1.3.6 and 2.1.4.1.5 mentioned above are also included in the scope of System Audit.

2.1.6. MIIs are advised to collaborate in developing a standardized definition of "near zero data loss" and submit the same to SEBI after taking approval from their respective SCOT.

2.2. **Business Continuity Plan (BCP) and Disaster Recovery (DR) framework – Limited Purpose Clearing Corporation (LPCC)**[4]

2.2.1. The LPCC has been permitted to have arrangements with any of the existing Clearing Corporations for the purposes of putting in place a BCP and DR mechanism, as per the framework placed at Para 1 in Annexure V.

2.3. **Standard Operating Procedure for handling of technical glitches by Market Infrastructure Institutions (MIIs) and payment of "Financial Disincentives" thereof**[5]

[4] Circular No. SEBI/HO/MRD2/DCAP/CIR/P/227 dated November 06, 2020

[5] Circular Nos. SEBI/HO/MRD1/DTCS/CIR/P/2021/590 dated July 05, 2021, SEBI/HO/MRD/TPD-1/P/CIR/2024/124 dated September 20, 2024 and SEBI/HO/MRD/TPD/CIR/P/2025/08 dated January 28, 2025

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

2.3.2. Considering the dependence of MIIs on technology and criticality of smooth functioning of their systems, specifying a pre-defined threshold for downtime of systems of MIIs becomes desirable to minimize instances of technical glitches at MIIs. For any downtime or unavailability of services, beyond such pre-defined time, there is a need to ensure that "Financial Disincentive" is paid by the MIIs. This will encourage MIIs to constantly monitor the performance and efficiency of their systems and upgrade/ enhance their systems etc. to avoid any possibility of technical glitches/disruption/disaster and restart their operations expeditiously in the event of glitch/disruption/disaster.

2.3.3. Accordingly, it has been decided that MIIs shall:

2.3.3.1. Follow the Standard Operating Procedure (SOP) for handling technical glitches as detailed at Annexure VI, and,

2.3.3.2. Comply with the "Financial Disincentive" structure as detailed at Annexure VII.

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

2.4. **Advisory for reporting of technical glitches**[6]

2.4.1. MIIs shall comply with the following regarding technical glitches resulting into business disruption, not being in the nature of a Disaster:

2.4.1.1. An MII, while reporting any technical glitch to its SCOT, must explicitly state if the said technical glitch has affected any member/participant/investor and if any complaint has been received by the MII in respect of the said technical glitch.

2.4.1.2. In case a technical glitch has affected any member/participant/investor and/or the MII has received any complaint from a member/participant/investor in this regard, the said technical glitch has to be necessarily reported to SEBI as a technical glitch resulting into business disruption.

2.4.1.3. If performance issue/slowdown/intermittent issues are observed beyond the specified time (viz. not in the nature of a Disaster), the same shall be considered as business disruption at the MII and the

[6] Email dated April 25, 2025 of SEBI on "Advisory for reporting of technical glitches"

concerned MII shall pay financial disincentive as per the extant regulatory framework.

2.4.1.4. Failure to pay such financial disincentive by the concerned MII (as mentioned at Para 2.4.1.3 above) could result in enforcement action by SEBI.

2.4.1.5. MIIs may suitably incorporate the aforesaid requirements in their Business Continuity Policy/Framework/Procedures.

2.5. **Measures to strengthen tracking and reporting of delay in pay-in/pay-out for rolling settlement**[7]

2.5.1. Following measures shall be put in place to strengthen tracking of intermediate activities in rolling settlement and reporting of settlement delays. This is without prejudice to financial disincentives, if any, emanating from delay in completion of pay-in/pay-out activities.

2.5.2. **For tracking of intermediate activities constituting rolling settlement**

2.5.2.1. CCs and Depositories may put in place systems to ensure:

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

2.5.2.3. Such intermediate activities are defined along with outer timelines for each activity after discussion with the concerned stakeholders such as members/participants, DVP agent, participating banks, other Market Infrastructure Institutions (MIIs) etc. to achieve final pay-in and pay-out within SEBI stipulated timelines.

2.5.2.4. Process flow and associated timelines, so decided, are intimated to all the stakeholders and delay in completion of any of these activities, should be traceable and attributable to one or more entity / MII, as the case may be.

[7] SEBI Email dated January 31, 2022

2.5.2.5. Procedures to handle various exceptions i.e. scenarios that could result in settlement delay are documented along with the steps to be taken towards completing settlement processes at the earliest in case of exceptions.

2.5.2.6. On the basis of the aforesaid, CCs and Depositories may separately prepare a Comprehensive Standard Operating Procedure (CSOP) which is mutually agreed upon by other CCs and Depositories as far as all the timelines and exception handling are concerned. This CSOP would be submitted to SEBI after approval of the Governing Boards of CCs and Depositories.

2.5.2.7. Further, the said CSOP shall also cover action points emanating from 8.4.3 below and would be reviewed periodically by the MIIs to incorporate any regulatory/system changes.

2.5.3. **For reporting of Delay in rolling settlement cycle**

2.5.3.1. In case of delay in completion of any of the intermediate activities beyond their pre-agreed time, the respective CCs/Depositories would inform the impacting CCs/Depositories regarding delay in completion of the intermediate activity at their end on immediate basis.

2.5.3.2. CCs shall intimate delay in settlement beyond the stipulated timelines for settlement for rolling settlement to SEBI (under intimation to depositories). This intimation should be given within one hour of such SEBI stipulated timelines and should inter-alia mention - reasons for delay, entity/MII responsible for the delay and likely completion time of the settlement process.

2.5.3.3. CCs and Depositories shall submit a separate report to their respective SCOT, on a monthly basis (replacing the existing joint monthly report), wherein following details are inter-alia provided:

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

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

of individual instances of settlement delay along with reasons thereof and corrective / preventive actions taken.

2.6. **Advisory on Security Patch Management Policy**[8]

All the MIIs are advised to ensure the following:

2.6.1. The security patch management policy is audited by an external auditor.

2.6.2. Appropriate changes, if necessary, are made to the existing policy on security patch management.

2.7. **Standard Operating Procedure for handling of Stock Exchange Outage and extension of trading hours thereof**[9,10]

2.7.1. If due to any technical reason or otherwise, continuous trading on stock exchanges is disrupted, it is of paramount importance that not only all market participants including other MIIs, are promptly informed about the outage but also the trading hours are extended, if required, so as to provide opportunity for smooth closure of intraday positions.

2.7.2. With a view to ensure that any outage at stock exchange(s) is handled in a harmonized and consistent manner, Standard Operating Procedure with regard to handling of such stock exchange outage in Cash Market, Equity Derivatives and Commodity Derivatives segment is detailed below.

Definition of Stock Exchange Outage

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

Reporting Requirements for outage

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

S No.	Communication to	Reporting
i.	Market Participants /	Immediate but not later than 15 minutes from occurrence of outage. Through

[8] SEBI Email dated September 12, 2022
[9] Circular No. SEBI/HO/MRD-TPD-1/CIR/P/2023/7 dated January 09, 2023
[10] Circular No. SEBI/HO/MRD/MRD-PoD-1/P/CIR/2024/62 dated May 27, 2024

	Trading Members / Other MIIs	broadcast message and by publishing on its website
ii.	SEBI	Immediate after occurrence of outage. Through an email to dedicated email id : techglitch@sebi.gov.in

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

I. Provisions applicable for Cash Market and Equity Derivatives

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

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

2.7.7. Affected stock exchange would restore operations to normalcy at the earliest including from the Disaster Recovery Site and carry out various activities, in terms of Para 2.1 and 2.3 of this Circular for MIIs.

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

Extension of trading hours in case of outage

2.7.9. If the trading on the affected stock exchange resumes to normalcy at least one hour (excluding 15 minutes of pre-opening session, if applicable) before the normal scheduled market closure, trading hours on that day for all stock exchanges would remain unchanged.

2.7.10. If the trading on the affected stock exchange does not resume to normalcy even one hour (excluding 15 minutes of pre-opening session, if applicable) before the scheduled market closure, trading hours for all stock exchanges would automatically get extended for additional one and half hours for that day and the same would be intimated by the affected stock exchange to market participants, other MIIs and SEBI latest by one hour fifteen minutes before the normal scheduled market closure. Subsequent to the communication from the affected stock exchange, the unaffected stock exchanges would also suitably

issue a notice with regard to extension of trading hours on their stock exchanges.

2.7.11. If the trading on the affected stock exchange does not resume to normalcy even 45 minutes (excluding 15 minutes of pre-opening session, if applicable) post normal scheduled market closure, in the case of extension of trading hours, no further trading would be allowed on the affected stock exchange for that day and other stock exchanges would continue to operate till the extended time provided at para 11 above to enable smooth closure/settlement of intraday positions. The affected exchange would have to suitably intimate the same to market participants, other MIIs and SEBI latest by 45 minutes post normal scheduled market closure.

2.7.12. If the occurrence of outage as mentioned in para 2.7.3 above, happens during the last trading hour of normal operation and latest before 15 minutes of normal scheduled market closure, trading hours for all stock exchanges would automatically get extended by one and half hours for that day and the same would be intimated by the affected stock exchange to market participants, other MIIs and SEBI immediately but not later than 10 minutes from the occurrence of outage. Subsequent to the communication from the affected stock exchange, the unaffected stock exchanges would also suitably issue a notice with regard to extension of trading hours on their stock exchanges.

2.7.13. Exchanges have to put in place a common close out policy to ensure uniform methodology of settlement of open positions, in case continuous trading didn't happen in Cash Market or Equity Derivative Segment of the exchange during last half an hour of trading for the day due to outage.

2.7.14. Extension of trading hours, if any, for Cash Market would result in equivalent extension of trading hours in Equity Derivative Segment and vice versa, provided trading hours at the start of the day are aligned for both Cash Market and Equity Derivative Segment. Further, Extension of trading hours in the Cash Market would also result in equivalent extension to other secondary market mechanisms conducted during trading hours such as Offer for Sale, Buy back etc.

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

S No	**Occurrence of outage**	**Event**	**Extension of trading hours**
1	In Equity Derivative Segment of exchange A	Normalcy in the said segment restored latest by 14:30	No extension of trading hours for exchange A and B

2	In Cash Market of exchange A	Start of Pre-opening latest by 14:15	No extension of trading hours for exchange A and B
3	Any time during the trading hours in Cash Market on exchange A	Failure to start Pre-opening by 14:15 on exchange A	Trading hours in Cash Market and Equity Derivative Segment of exchange A and B extended till 17:00 and announcement in this regard to be made latest by 14:15 by the affected stock exchange. Note that such announcement is to be made on the basis of assessment by stock exchange on the likely resumption of normalcy.
		Failure to start Pre-opening by 16:00 on exchange A	No trading permitted in Cash Market on exchange A for the day. Equity Derivative Segment on exchange A and Cash Market and Equity Derivative Segment on exchange B would continue to trade till 17:00. The affected stock exchange to announce latest by 16:15.
4	At 15:05 on exchange A in Cash Market		Trading hours in Cash Market and Equity Derivative Segment of exchange A and B extended till 17:00 and announcement to be made by affected stock exchange within 10 minutes of occurrence of outage i.e. by 15:15
5	At 15:16 on exchange A in Cash Market		No extension of trading hours for exchange A and B

II. Provisions applicable for Commodity Derivatives Segment

2.7.16. If outage occurs on one exchange, market hours shall remain unchanged on unaffected exchange/s.

2.7.17. Affected stock exchange would restore operations to normalcy at the earliest including from the Disaster Recovery Site and carry out various activities, in terms of Para 2.1 and 2.3 of this Circular for MIIs.

2.7.18. The provisions for handling exchange outage for commodity derivatives segment, are as follows:

A. For contracts/products traded up to 5 pm / 9 pm

2.7.19. If trading resumes to normalcy at least 30 minutes before scheduled market closure (excluding 15 minutes of prior intimation time), trading hours would remain unchanged on that exchange i.e., market participants will have to be

intimated latest by 4:15 pm or 8:15 pm regarding resumption of trading by 4:30 pm or 8:30 pm.

2.7.20. The intimation to re-start trading can be sent latest till 4:45pm or 8:45pm, as the case may be. The intimation shall, inter-alia, inform that trading shall commence from 5 pm or 9 pm for a duration of 30 minutes i.e., extended trading hours would be till 5:30pm or 9:30pm. The intimation shall also include details as to when investors can / should login to modify their position.

2.7.21. If intimation is not sent to market participants by 4:45pm or 8:45pm, then there shall be no extension of trading hours.

2.7.22. The above conditions are illustrated as under:

Table 1: For contracts traded up to 5:00 PM

Intimation to market participants	Resumption of trading	Extended market hours
4:15PM	4:30PM - 5 PM	NA
4:45 PM	5:00PM - 5:30 PM	30 mins
After 4:45 PM	NA	NA

Table 2: For contracts traded up to 9:00 PM

Intimation to market participants	Resumption of trading	Extended market hours
8:15PM	8:30PM - 9 PM	NA
8:45 PM	9:00PM - 9:30 PM	30 mins
After 8:45 PM	NA	NA

B. For contracts/products traded up to 11:30pm / 11:55 p.m.

2.7.23. If trading resumes to normalcy at least 30 minutes before scheduled market closure (excluding 15 minutes of prior intimation time), trading hours would remain unchanged on that exchange, i.e., market participants will have to be intimated by 10:45pm or 11:10pm regarding resumption of trading by 11:00pm or 11:25pm.

2.7.24. The intimation to re-start trading can be sent latest until 11:10pm. The intimation shall, inter-alia, inform that trading shall commence from 11:25pm for a duration of 30 minutes i.e., extended trading hours would be till 11:55pm. The intimation shall also include details as to when investors can / should login to modify their position.

2.7.25. If intimation is not sent to market participants by 11:10pm, then there shall be no extension of trading hours.

2.7.26. The above conditions are illustrated as under:

Table 3: For contracts traded up to 11:30PM

Intimation to market participants	Resumption of trading	Extended market hours
10:45 PM	11:00 PM - 11:30 PM	NA
11:10PM	11:25 PM - 11:55 PM	30 mins
After 11:10PM	NA	NA

Table 4: For contracts traded up to 11:55 PM

Intimation to market participants	Resumption of trading	Extended market hours
11:10 PM	11:25 PM - 11:55 PM	NA
After 11:10PM	NA	NA

2.8. **Testing Framework for the Information Technology (IT) Systems of the Market Infrastructure Institutions (MIIs)[11]**

2.8.1. In order to assist MIIs in performing thorough risk assessment before deploying any IT systems in production/ live environment, MIIs are hereby directed to ensure the following requirements while establishing the testing framework of their IT systems/applications:

2.8.1.1. All MIIs should do extensive testing, validation and documentation whenever new systems/ applications or changes to existing systems/applications are introduced before the deployment in production/live environment

2.8.1.2. A comprehensive methodology for system testing, functional testing, application security testing should be established and the same shall be approved by SCOT of respective MIIs. The scope of testing shall, inter-alia, cover business logic, system function, security controls and system performance under load and stress conditions. Any dependency on the existing systems shall be properly tested.

2.8.1.3. Testing should be carried out in a separate environment that replicates/mirrors the production environment in order to minimize any disruption.

2.8.1.4. All MIIs shall have the practice of traceability matrix to ensure that the test plan covers all intended functionality of the IT system and application.

2.8.1.5. All MIIs shall adopt the practice of using automated testing techniques to run the test cases automatically, which may increase the depth and scope of tests and ultimately help to improve the software quality.

2.8.1.6. All MIIs shall establish policy/procedures on the use of third party systems/applications/software codes to ensure these systems are subject to review and testing before they are integrated with the systems of the MIIs.

[11] Circular No. SEBI/HO/MRD/TPD/P/CIR/2023/65 dated May 05, 2023

2.8.1.7. All MIIs shall ensure that core code components operate as intended and do not produce unintended consequences. Further, any new code shall not have any impact on the existing functionality. All MIIs shall also ensure that Application Programming Interface Testing is done so that the concerned application can interact with other applications without causing disruptions of any kind.

2.8.1.8. All MIIs should perform regression testing for changes (e.g. enhancement, rectification, etc.) to an existing IT system to validate that it continues to function properly after the changes have been implemented. After fixing the defects found during the testing, all MIIs shall perform regression testing again to ensure that other existing functionalities are not affected during fixing the defects. All MIIs shall explore to capture the automated test cases so that regression testing can be performed multiple times with much wider coverage test cases in a short time.

2.8.1.9. All MIIs may institute tools to measure test/code coverage to assess comprehensiveness of the test.

2.8.1.10. All issues identified from testing, including system defects or software bugs, should be properly tracked and remediated immediately. Major issues that could have an adverse impact on the MII should be reported to their SCOT and addressed prior to deployment to the production environment.

2.8.1.11. All MIIs should ensure that the results of all testing, including results of User Acceptance Testing (UAT), that was conducted, are documented in the test report. The same shall be checked by the auditor during System and Network Audit.

2.8.1.12. All MIIs shall periodically conduct non-functional testing such as volume testing, resilience testing, scalability testing, performance testing, stress testing, application security testing, BCP testing, negative/destructive testing etc. for all IT systems/applications throughout their lifecycle (pre-implementation, post implementation, after changes).

2.8.1.13. All MIIs shall perform white box testing or structural testing, which shall inter-alia include analyzing data flow, control flow, information flow, coding practices, exception and error handling within the system.

2.8.2. The MIIs are required to take necessary steps to put in place systems for implementation of the provisions on testing framework, including necessary amendments to the relevant bye-laws, rules and regulations, if any. The MIIs are advised to submit the testing framework of all their IT systems after approval of SCOT.

2.9. **Business Continuity for Clearing Corporations through Software as a Service (SaaS) Model (except Commodity Derivatives Exchanges and Clearing Corporations)[12]**

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

2.9.2. Non-availability of RMS, which is a critical system of CC, poses a major risk to the continuity of trading on stock exchanges. In order to further manage disruptions impacting availability of RMS, it is proposed to have another contingency measure in place under Software as a Service (SaaS) model. The framework in the first phase would operate for existing interoperable segments of CCs (Cash Market, Equity Derivatives Segment, Currency Derivatives) as follows:

Outline of SaaS model for RMS:

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

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

2.9.4.1. The SaaS-RMS instance would be designed to accept the trade data from exchanges; online collateral, positions etc. from the CC(s) and depository data as required from depositories. The client CC would carry out all the functions related to online real time risk management at the SaaS-RMS. This would ensure that if the SaaS-RMS is invoked by client CC, it would be in a ready state to take over operations.

2.9.4.2. Responsibility of service provider CC would be to provide the functioning software for RMS and that for other associated processes to the client CC. Beyond that, it would be responsibility of the client CC to operate SaaS-RMS in normal course and on the day it is invoked. Further, client CC would put in place systems to detect

[12] SEBI/HO/MRD/TPD/P/CIR/2023/192 dated December 20, 2023

latency/performance issue of SaaS-RMS to flag off such anomalies to the concerned MII(s).

2.9.4.3. Each CC shall also make necessary arrangements for members to login to SaaS-RMS through a portal and view/add collateral and its utilization etc. in case SaaS-RMS is invoked by CC.

2.9.4.4. As the key purpose of the exercise is to ensure ability to risk manage trades, all the functions pertaining to risk management/collateral shall be made available by the client CC in the SaaS-RMS i.e.:

2.9.4.4.1. Intraday risk management of trades
2.9.4.4.2. Real time computation of margins and member utilization
2.9.4.4.3. Violation intimation to Exchanges
2.9.4.4.4. Response to Exchanges for orders of members in RRM
2.9.4.4.5. Online Custodial Participant Modifications / CP confirmations
2.9.4.4.6. Collateral addition by members
2.9.4.4.7. Receipt of Margin pledge / re-pledge data
2.9.4.4.8. Sending Margin pledge / re-pledge data
2.9.4.4.9. Member interface for Margin display, Custodial confirmations and Collateral addition/ allocation un-allocation
2.9.4.4.10. Handling of Early Pay-In (EPI) instructions

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

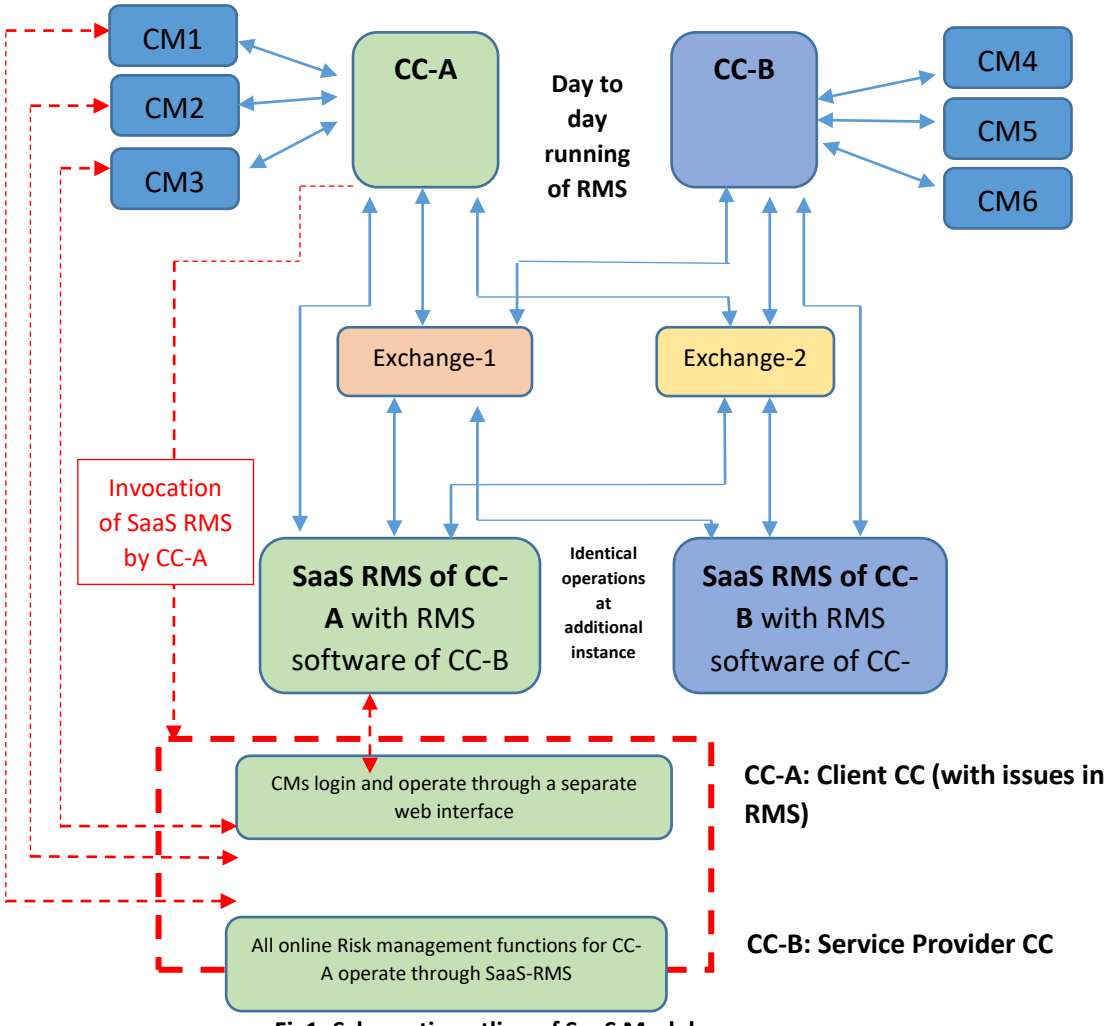


Fig1: Schematic outline of SaaS Model

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

2.9.6.1. In normal conditions, all the RMS related activities are replicated online by both CCs in the SaaS-RMS. CMs connect to CCs through normal web interface for collateral, positions related query, updates etc.

2.9.6.2. Due to certain issues / malfunctioning, once CC-A decides to invoke SaaS-RMS viz. designed using RMS software of CC-B, the RMS functioning to resume by CC-A through SaaS-RMS within the timelines stipulated in the instant circular.

2.9.6.3. CMs of CC-A to login and operate through a separate interface provided by CC-A.

2.9.7. On the basis of test runs carried out by CCs on a working model of Saas-RMS implemented by CCs, following timelines are stipulated:

2.9.7.1. A CC to take decision to shift operations to SaaS-RMS within 30 minutes of occurrence of its inability to do online real time risk management of trades at its site of functioning.

2.9.7.2. Within 30 minutes of the above, all allied activities such as sending violation messages to exchanges, intimating details of portal to interact with SaaS-RMS to the Clearing Members etc. to be activated through SaaS-RMS.

2.9.7.3. Mock session of SaaS-RMS to be carried out at least once in a quarter to familiarize and train members.

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

2.9.8.1. To enter into an agreement laying down the roles and responsibilities of each of the entities (i.e. exchange, CCs, depositories etc.) with regard to functioning of SaaS-RMS as envisaged

2.9.8.2. To prepare Standard Operating Procedures covering various operational issues and edge cases related to functioning of SaaS-RMS

2.9.8.3. To enhance existing Interoperability Agreement to clearly demarcate roles and responsibilities of exchanges and CCs in detecting and addressing scenarios causing delay in sending/receiving the transactions data from exchanges to CCs in real time

2.9.9. The MIIs are also directed to take necessary steps to put in place requisite infrastructure and systems for implementation of the provisions on SaaS, including necessary amendments to the relevant bye-laws, rules and

regulations and bring these provisions to the notice of their members and also disseminate the same on its website.

2.9.10. Considering the above, Stock exchanges and CCs are advised to submit their revised Business Continuity Policy to SEBI.

2.10. **Business Continuity for Interoperable Segments of Stock Exchanges** [13]

2.10.1. In case of outage of a trading venue (i.e. stock exchange) during trading hours, the participants with open positions would be exposed to price risk on such open positions, as there could be material news flow during that time. In such a case, the multi exchange set up along with interoperability among Clearing Corporations could be leveraged to provide an alternative trading venue to end investors. In this regard, following has been decided for the interoperable segments of stock exchanges (i.e. Cash Market/ Equity Derivatives/ Currency Derivatives/ Interest Rate Derivatives etc.):

2.10.1.1. Common scrips, derivatives on single stocks or correlated indices, currency derivatives segment and interest rate derivatives:

If identical or correlated trading products are available on another trading venue, then participants can hedge their open positions by taking offsetting positions in identical or correlated indices on other exchange. Further, as these segments are interoperable, taking offsetting positions in other trading venue would net off such open positions for end clients and release the margin. Hence, no separate treatment is required for such category of products.

2.10.1.2. Scrips exclusively listed on an exchange:

To ensure continuity, exchanges may create reserve contracts for scrips (i.e. exclusively listed scrips on other exchange) and single stock derivatives not traded on their exchange (and available on other exchange), to be invoked at the time of outage on the other exchange.

2.10.1.3. Index derivatives products not having correlated index derivatives products on another exchange:

Exchange which does not have a highly correlated index derivatives product with one available on other exchange may consider creating such an index and introducing derivatives contracts on it, in line with extant Regulatory provisions. The aforesaid would provide an avenue to hedge positions in index derivatives products of an exchange that suffered an outage.

2.10.1.4. Intimation to SEBI and Alternative Trading Venue:

[13] SEBI/HO/MRD/TPD/P/CIR/2024/167 dated November 28, 2024

The affected exchange should comply with extant Regulatory requirements with regard to handling of technical glitch/ outage and intimate about the invocation of the instant business continuity mechanism to the alternative trading venue and SEBI within 75 minutes of occurrence of impact. The alternative trading venue would invoke the business continuity plan as per the Standard Operating Procedure (SOP) within 15 minutes from such intimation.

2.10.2. Upon discussion with exchanges, it has been decided that to begin with, NSE would act as an alternative trading venue for BSE and vice-a-versa. Both exchanges would prepare a joint SOP that would include plan to be invoked at the time of outage on one exchange along with flow of activity involving the affected exchange and its alternative trading venue and roles/responsibility of each of them. Further, the SOP shall also cover changes, if any, in the systems of stock brokers / CCs to implement the measures mentioned at para 2.10.1 above for end investors.

2.11. **Advisory on Business Continuity and Disaster Recovery[14]**

2.11.1. MIIs shall ensure the following:

2.11.1.1. MIIs shall place the information about End of Life ("EOL")/End of Support ("EOS") status of their IT assets before their SCOT on a quarterly basis. MIIs shall have SOPs to replace the IT systems that have reached EOL. Further, MIIs should not use IT systems that have reached EOS as they would not receive bug fixes, security patches or any other updates from the OEMs.

2.11.1.2. MIIs are advised to perform proper vendor risk assessment at the time of on boarding as well on a periodic basis as part of ongoing monitoring to manage any potential risks throughout the lifecycle of a third-party service relationship.

2.11.1.3. MIIs are advised to create the provision of offline backups of data of any application at PDC and DRS before deployment of same in production environment.

[14] Email dated July 29, 2025 of SEBI on "Action points arising out of meeting of TAC held on March 27, 2025 w.r.t system and network audit reports submitted by MIIs"

3. CYBER SECURITY AND CYBER RESILIENCE

3.1. Cyber Security and Cyber Resilience framework – Limited Purpose Clearing Corporation (LPCC)[15]

3.1.1. The framework governing arrangements of LPCC with existing Clearing Corporations for the purpose of Cyber Security is placed at Para 2 in **Annexure V**.

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

3.2.1. MII shall take necessary steps to ensure that its website(s) are resilient to cyber-attack(s).

3.2.2. Redundant websites: MII shall host its website(s) at multiple DNS (Domain Naming Servers) and hosts. MII shall put-in place suitable systems to switch to alternate website(s) hosted on a different DNS / hosts in the event of a cyber-attack on its primary website(s) and at the same time, shall take necessary steps to recover from the cyber-attack on the its primary website(s).

3.2.3. Web Application Firewall (WAF): MII shall mandatorily deploy Web Application firewalls of demonstrated capabilities.

3.2.4. Continuous monitoring of the website(s): MII shall deploy suitable and adequate resources for 24x7 monitoring of its website(s), including monitoring of their website(s) through the SOCs (Security Operations Center).

3.2.5. MII shall periodically conduct penetration testing of its website(s) and related systems, at the minimum, once in a calendar year.

3.2.6. In cases where services of 3rd party vendors / service providers are availed by the MII for hosting of its website(s) and for other related areas, MII shall ensure that the cyber security and resilience framework of such 3rd party vendors / service providers are as per the requirements specified by SEBI for MIIs. Further, MII shall include audit of the cyber security and resilience framework of such 3rd party vendors / service providers (limited to the services availed by MIIs) in the scope of its annual system audit.

3.2.7. MII shall implement the principles mentioned in the 'Guidelines for Indian Government Websites' developed by National Informatics Centre (NIC) and adopted by Department of Administrative reforms and Public Grievances (DARPG) on the areas of 'Website Hosting', 'Website Management', 'Development', etc. MII shall refer to the updates to the said

[15] Circular No. SEBI/HO/MRD2/DCAP/CIR/P/227 dated November 06, 2020

guidelines from time to time. The said guidelines are currently available at https://guidelines.india.gov.in/introduction/.

3.2.8. MII shall frame and implement a Web Server Security Policy that should cover Network and Host Security Policy, Web Server Backup and Logging Policy, Web Server Administration and Updation Policy, Classification of documents to be published on Web Server, Password Management Policy, Encryption Policy, and Physical Security

3.2.9. In addition to the above, MIIs shall ensure implementation of the following:

3.2.9.1. MIIs shall advise their auditors to give additional emphasis on the Application Security audit.

3.2.9.2. MIIs shall include suitable IT / Cyber security related certifications requirements in the criteria for selection of software developers / vendors.

3.2.9.3. MIIs shall ensure that their software vendors undertake security audit of their systems on a periodic basis (at least once a year).

3.3. Bolstering Cyber Resiliency[16]

3.3.1. In addition to the current detection and prevention tools deployed at the MIIs for Network Traffic Analysis and other SIEM solutions, MIIs should start using User and Entity Behaviour Analytics (UEBA) tools for combating cyber threats.

3.4. Cyber Security and Cyber Resilience framework of MIIs[17]

3.4.1. With the view to strengthen the Cyber Security and Cyber Resilience framework of MIIs, particularly in respect of monitoring of cyber threats and cyber resiliency, MIIs shall have a Cyber Security Operation Center (C-SOC) that would be a 24x7x365 set-up manned by dedicated security analysts to identify, respond, recover and protect from cyber security incidents.

3.4.2. The C-SOC shall function in accordance with the Cyber Security and Cyber Resilience Framework (CSCRF) for Regulated Entities (SEBI Circular Number SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024) prescribed by SEBI. Illustrative list of broad functions and objectives to be carried out by a C-SOC are mentioned hereunder:

3.4.2.1. Prevention of cyber security incidents through proactive actions:

[16] SEBI Email dated November 11, 2017 captioned Bolstering Cyber Resiliency
[17] Refer SEBI Circular CIR/MRD/CSC/148/2018 dated December 07, 2018

3.4.2.1.1. Continuous threat analysis,
3.4.2.1.2. Network and host scanning for vulnerabilities and breaches,
3.4.2.1.3. Countermeasure deployment coordination,
3.4.2.1.4. Deploy adequate and appropriate technology at the perimeter to prevent attacks originating from external environment and internal controls to manage insider threats. MIIs may implement necessary controls to achieve zero trust security model.

3.4.2.2. Monitoring, detection, and analysis of potential intrusions / security incidents in real time and through historical trending on security-relevant data sources.
3.4.2.3. Response to confirmed incidents, by coordinating resources and directing use of timely and appropriate countermeasures.
3.4.2.4. Analysis of the intrusions / security incidents (including Forensic Analysis and Root Cause Analysis) and preservation of evidence.
3.4.2.5. Providing situational awareness and reporting on cyber security status, incidents, and trends in adversary behavior to appropriate organizations including to CERT- In and NCIIPC.
3.4.2.6. Engineer and operate network defense technologies such as Intrusion Detection Systems (IDSes) and data collection / analysis systems.
3.4.2.7. MIIs to adopt security automation and orchestration technologies in C-SOC to automate the incident identification, analysis and response as per the defined procedures.

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

3.4.3.1. In order to detect intrusions / security incidents in real time, the C-SOC should monitor and analyze on a 24x7x365 basis relevant logs of MII's network devices, logs of MII's systems, data traffic, suitable cyber intelligence (intel) feeds sourced from reliable vendors, inputs received from other MIIs, inputs received from external agencies such as CERT-In, etc. The cyber intelligence (intel) feeds may include cyber news feeds, signature updates, incident reports, threat briefs, and vulnerability alerts.
3.4.3.2. To this end, appropriate alert mechanisms should be implemented including a comprehensive dashboard, tracking of key security metrics and provide for cyber threat scorecards.
3.4.3.3. The C-SOC should conduct continuous assessment of the threat landscape faced by the MII including undertaking periodic VAPT (Vulnerability Assessment and Penetration Testing).
3.4.3.4. The C-SOC should have the ability to perform Root Cause Analysis, Incident Investigation, Forensic Analysis, Malware Reverse Engineering,

etc. to determine the nature of the attack and corrective and/or preventive actions to be taken thereof.

3.4.3.5. The C-SOC should conduct periodic (at the minimum quarterly) cyber attack simulation to aid in developing cyber resiliency measures. The C-SOC should develop and document mechanisms and standard operating procedures to recover from the cyber-attacks within the stipulated RTO of the MII. The C-SOC should also document various scenarios and standard operating procedures for resuming operations from Disaster Recovery (DR) site of MII.

3.4.3.6. The C-SOC should conduct periodic awareness and training programs at the MII and for its members / participants / intermediaries with regard to cyber security, situational awareness and social engineering.

3.4.3.7. The C-SOC should be capable to prevent attacks similar to those already faced. The C-SOC should also deploy multiple honey pot services which are dynamic in characteristics to avoid being detected as honey pot by attackers.

3.4.4. As building an effective C-SOC requires appropriate mix of right people, suitable security products (Technology), and well-defined processes and procedures (Processes), an indicative list of areas that MIIs should consider while designing and implementing a C-SOC are as follows:

3.4.4.1. The MII shall ensure that the governance and reporting structure of the C-SOC is commensurate with the risk and threat landscape of the MII. The C-SOC shall be headed by the Chief Information Security Officer (CISO) of the MII. The CISO shall be designated as a Key Managerial Personnel (KMP) and relevant provisions relating to KMPs as prescribed by SEBI, shall apply to the CISO.

3.4.4.2. While the CISO is expected to work closely with various departments of MIIs, including MII's Network team, Cyber Security team and Information Technology (IT) team, etc., the reporting of CISO shall be directly to the MD & CEO of the MII.

3.4.4.3. The roles and responsibilities of CISO may be drawn from Ministry of Electronics and IT notification No. 6(12)/2017-PDP-CERT-In dated March 14, 2017.[18]

3.4.4.4. The C-SOC should deploy appropriate technology tools of adequate capacity to cater to its requirements. Such tools shall, at the minimum, include Security Analytics Engine, Malware detection tools, Network and User Traffic Monitoring and Behavior Analysis systems, Predictive Threat Modelling tools, Tools for monitoring of System parameters for

[18] CISO roles & responsibilities - Ministry of Electronics and IT notification No. 6(12)/2017-PDP-CERT-In dated March 14, 2017

critical systems / servers, Deep Packet Inspection tools, Forensic Analysis tools, etc.

3.4.4.5. Each MII is advised to formulate a Cyber Crisis Management Plan (CCMP) based on its architecture deployed, threats faced and nature of operations. The CCMP should define the various cyber events, incidents and crisis faced by the MII, the extant cyber threat landscape, the cyber resilience envisaged, incident prevention, cyber crisis recognition, mitigation and management plan. The CCMP should be approved by the respective Standing Committee on Technology / IT- Strategy Committee of the MIIs and the governing board of the MII. The CCMP should be reviewed and updated as per frequency defined in CSCRF.

3.4.4.6. The C-SOC should have well-defined and documented processes for monitoring of its systems and networks, analysis of cyber security threats and potential intrusions / security incidents, usage of appropriate technology tools deployed by C-SOC, classification of threats and attacks, escalation hierarchy of incidents, response to threats and breaches, and reporting (internal and external) of the incidents.

3.4.4.7. The C-SOC should employ domain experts in the field of cyber security and resilience, network security, data security, end-point security, etc.

3.4.4.8. The MIIs are also advised to build a contingent C-SOC at their respective DR sites with identical capabilities w.r.t. the primary C-SOC in line with Para 2.1. Additionally, the MIIs should perform monthly live-operations from their DR-C-SOC.

3.4.4.9. The C-SOC should document the cases and escalation matrices for declaring a disaster.

3.4.5. In view of the feedback received from MIIs, it has been decided that MIIs may choose any of the following models to set-up their C-SOC:

(i) MII's own C-SOC manned primarily by its internal staff
(ii) MII's own C-SOC, staffed by a service provider, but supervised by a full time staff of the MII (Refer to Clause 3.4.5.3)
(iii) C-SOC that may be shared by the MII with its group entities (that are also SEBI recognized MIIs)
(iv) C-SOC that may be shared by the MII with other SEBI recognized MII(s).

3.4.5.1. The responsibility of cyber security of an MII, adherence to business continuity and recovery objectives, etc. should lie with the respective MII, irrespective of the model adopted for C-SOC.

3.4.5.2. The respective risk committee(s) of the MII should evaluate the risks of outsourcing the respective activity.

3.4.5.3. The MII may outsource C-SOC activities in line with the guidelines as given in Annexure VIII.

3.4.6. A report on the functioning of the C-SOC, including details of cyber-attacks faced by the MII, major cyber events warded off by the MII, cyber security breaches, data breaches should be placed on a quarterly basis before the board of the MII.

3.4.7. The system auditor of the MII shall audit the implementation of the aforesaid guidance in the annual system audit of the MII. The Scope and/or Terms of Reference (ToR) of the annual system would accordingly be modified to include audit of the implementation of the aforementioned areas.

3.4.8. Further, in continuation to the requirement specified at Part II: Guidelines in the SEBI Circular Number SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024 on Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs), the C-SOC shall share relevant alerts and attack information with members / participants / intermediaries of the MII, other MIIs, external cyber response agencies such as CERT-In, and SEBI.

3.5. **Reporting for Artificial Intelligence (AI) and Machine Learning (ML) applications and systems offered and used by Market Infrastructure Institutions (MIIs)**[19]

Scope definition

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

3.5.2. Technologies that are considered to be categorized as AI and ML technologies in the scope of this circular, are explained in Annexure IX.

Regulatory requirements

3.5.3. All MIIs shall fill in the AI / ML reporting form (Annexure X) in respect of the AI or ML based applications or systems as defined in Annexure IX offered or used by them, and submit the same in soft copy only at

[19] SEBI Circular SEBI/HO/MRD/DoP1/CIR/P/2019/24 dated January 31, 2019

AI_MII_SE@sebi.gov.in (for Stock Exchanges)/ AI_MII_DEP@sebi.gov.in (for Depositories)/ AI_MII_CC@sebi.gov.in (for Clearing Corporations) to SEBI on a quarterly basis within 15 days of the expiry of the quarter.

3.6. **Standard Operating Procedure for reporting of Cyber Security breaches, incidents and deficiencies and for imposition of "Financial Disincentive" on Market Infrastructure Institutions (MIIs)** [20]

3.6.1. MIIs shall address cyber security deficiencies and breaches in a timely manner by taking appropriate corrective actions. In case of non-compliance with regulatory framework for cyber security and cyber resilience, a "Financial Disincentive" on MIIs can be levied in the event of the following cases:

3.6.1.1. Non-compliance with the extant cyber security regulations and guidelines resulting in cyber security breaches, cyber-attacks, cyber security deficiencies or any other cyber security incidents

3.6.1.2. Lackadaisical approach or undue delay in addressing cyber security deficiencies and breaches

3.6.1.3. Non-reporting/ delay in reporting a cyber security incident/breach

The intent of this financial disincentive is to encourage the MIIs to constantly monitor the performance of their systems and upgrade/ enhance their systems so as to eliminate cyber security deficiencies and prevent or minimize the possibility of a cyber security breach.

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

Definitions

3.6.3. "*Cyber security deficiency*" shall be defined as a loophole, vulnerability or non-compliance observed in

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

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

[20] SEBI Letter SEBI/HO/MRD/CSC/OW/P/2019/22202/1 dated August 28, 2019

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

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

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

3.6.6. "*Information security practices*" shall be defined as implementation of cyber security policies and standards in order to minimize the cyber security incidents and cyber security breaches.

3.6.7. "*Cyber security policy*" shall be defined as a set of documented business rules and processes for protecting information and the computer resource.

3.6.8. "*Cyber security protocol*" shall be defined as the official procedure or system of rules governing the cyber security operations of a MII. The cyber security protocol is usually as subset of the cyber security policy.

3.6.9. "*Operational guidelines*" refers to any additional set of rules and procedures issued internally by a MII that compliments its cyber security protocol and information security practices.

Reporting Requirements

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

Sl. No.	Issue	Reporting
1.	Cyber Security	• CERT-In • SEBI's Cyber Security Cell

Sl. No.	Issue	Reporting
	Breach / Incident	• Standing Committee on Technology of the MII • Governing Board of the MII
2.	Cyber Security Deficiencies	• Standing Committee on Technology of the MII • Governing Board of the MII • SEBI's Cyber Security Cell

Cases for levy of "Financial Disincentive"

3.6.11. The "Financial Disincentive" shall be levied in the following cases:

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

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

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

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

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

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

3.6.11.2. Cyber Security deficiencies occurring on account of non-compliance of SEBI cyber security policies and guidelines observed during biannual cyber security audits mandated by SEBI or reports from other agencies.

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

3.6.11.3. A cyber security breach / incident should be reported as soon as it is discovered as per the reporting structure specified in Clause 3.6.10 A

"Financial Disincentive" of Rs.10,00,000/- (ten lakhs) shall be levied on those MIIs that

3.6.11.3.1. Do not report a cyber security breach/incident, or
3.6.11.3.2. Delay the reporting of the cyber security breach/incident

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

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

3.6.12. Notwithstanding the reporting structure mentioned in Clause 3.6.10 above, the penalties would start being levied by SEBI in Clause 3.6.11 as mentioned above.

Proceeds to be credited to SEBI's IPEF

3.6.13. Further, with a view to making such "Financial Disincentives" effective and meaningful, the amount realized from the same shall be credited to the "Investor Protection and Education Fund" of SEBI in accordance with Section 11(1) of SEBI Act, 1992 read with Regulation 4(1)(m) of the Securities and Exchange Board of India (Investor Protection and Education Fund) Regulations, 2009.

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

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

3.7. Advisory on Cyber Audit and VAPT[21]

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

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

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

3.7.3. The cyber audit report is to be submitted in the Standardized format. Please refer to CSCRF for the said standardised format.

3.7.4. Along with cyber audit reports, all MIIs are required to submit to SEBI the comments of their SCOT and Governing Board.

3.7.5. Scope of cyber audit shall also include testing the functional efficacy of the SOC.

3.7.6. VAPT exercise shall cover all possible ingress and egress points including broker ICT setup, co-location facility etc.

3.7.7. All MIIs shall conduct Periodic Training for the concerned employees regarding Cyber Security in line with CSCRF and the same has to be checked by the Auditors during cyber audit.

3.7.8. The audit report shall include control wise compliance of all SEBI circulars/advisories along with the evidences.

3.7.9. All MIIs are advised to include the directions issued by SEBI pursuant to discussion in HPSC-CS in their regular bi-annual cyber audit.

3.7.10. In order to ascertain the compliance of identification of critical assets as per CSCRF, process of identification of critical assets and its implementation should be assessed during cyber audit.

3.7.11. For minimum baseline standards followed for conducting VAPT, please refer to CSCRF.

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

3.8. Advisory on Cyber security and Cyber resilience

With regard to the cyber security preparedness, MIIs shall strictly follow provisions related to SOC Operations, Network Security Management, VAPT (including those in Annexure-L), Change Management, Backup Management, Zero Trust, Physical Security etc. as prescribed in CSCRF. Additionally, MIIs shall :

[21] SEBI Email dated December 28, 2022

3.8.1. physically segregate the network implemented for doing various kind of automation for physical security of building vis-à-vis networks implemented for core activities.

3.8.2. ensure that all identified critical high impact vulnerabilities in their IT environment shall be closed on an urgent basis.

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

4. CAPACITY PLANNING

4.1. Capacity planning and Real Time Performance Monitoring framework of Market Infrastructure Institutions(MIIs)[22], [23]

4.1.1. Stock exchanges, Clearing Corporations and Depositories (i.e. MIIs) are advised to ensure the following requirements while formulating the framework of capacity planning and real time performance monitoring of their Critical Information Technology (IT) systems and supporting infrastructure components:

4.1.1.1. Capacity planning methodology should be proactive, future ready and developed to help estimate/forecast future projected capacity requirements to support business activities and minimize the risk of service disruption (taking into account trend analysis of system utilization, historical volume, maximum allowed volume to all members/participants taken together such as number of orders/messages per second, projection of customer growth/transaction volume, system performance issues, implication of any new business initiatives, possible surge in transaction volume etc.) Details of the methodology adopted by MIIs shall be submitted to SEBI after taking approval of their Standing Committee on Technology (SCOT) and Governing Board.

4.1.1.2. All MIIs should ensure adequate system capacity in place to handle high volumes to ensure high level of service availability.

4.1.1.3. The installed capacity shall be at least 1.5 times (1.5x) of the projected peak load. However for Commodity Derivatives Segment, the installed capacity shall be least 2 times (2x) of the projected peak load.

4.1.1.4. The projected peak load shall be calculated for the next 60 days based on the sustained peak load trend of the past 180 days and other relevant factors including futuristic factors as mentioned at paragraph 11.1.1.1 above. However, MIIs may also calculate the projected peak load for time duration shorter than 60 days. The exact duration of sustained peak load to be considered by MIIs to calculate the projected peak load shall be decided based on the consultation with their SCOT. However, the outer limit for sustained peak load shall be 10 seconds for Stock Exchanges and Clearing Corporations and 5 minutes for Depositories.

4.1.1.5. MIIs shall conduct comprehensive stress testing on quarterly basis to identify the impact on throughput/performance/latency metrics when

[22] Circular No. SEBI/HO/MRD/TPD/CIR/P/2024/171 dated December 10, 2024
[23] Circular No. HO/47/13/14(1)2026-MRD-TPD1/I/4755/2026 dated February 11, 2026

compared to lean period by stressing the existing load scenarios to various multiples.

4.1.1.6. MIIs shall ensure that application design should have horizontal and vertical scalability and the same shall be tested on periodic basis.

4.1.1.7. MIIs shall have guidelines/Standing Operating Procedures (SOPs) to identify and understand the performance of each application/process, capacity, utilization of each individual IT component, within the entire system/network architecture, used to support their IT services.

4.1.1.8. While devising the capacity planning and real time performance monitoring methodology, MIIs should not consider each IT component/application/process in isolation and must consider inter-dependency of the IT components/applications/processes.

4.1.1.9. All IT systems shall be considered in this process which shall, inter-alia, include network, hardware, software, security devices, network devices, memory utilization, CPU utilization, disks, network links, third party vendor systems, supporting infrastructure etc., and shall be adequately sized to meet the capacity and real time performance requirements to support the business activities of the MII.

4.1.1.10. All MIIs shall implement automated performance monitoring and alert system covering all their critical applications/activities/IT components to continuously monitor the real time performance of processes/applications and utilization of its system resources at each IT component level against a set of pre-defined thresholds. These thresholds should enable the MIIs to do early detection of any possible performance issue, slowness etc. and should be set accordingly. A dedicated team should monitor such alerts and SOPs should be put in place to address such alerts in a timely manner to ensure performance of systems/applications/processes of MIIs. The said performance monitoring and alert system shall be reviewed on quarterly basis.

4.1.1.11. Alerts generated from the monitoring and detection systems shall be dealt proactively including necessary actions such as infrastructure up-gradation, addition of IT resources etc. shall be taken immediately to address the issue effectively.

4.1.1.12. All MIIs shall maintain an asset register of all IT components and monitor their usage on a continuous basis. MIIs shall examine and establish an appropriate threshold on utilization of each component. If actual utilization of any component of MII exceeds the threshold over a period as defined by MII, immediate action shall be taken to enhance the capacity. The threshold must be reviewed and approved by SCOT of the MII.

4.1.1.13. In general, if actual capacity utilization of any component of Stock Exchanges and Clearing Corporations exceeds 75% of the installed capacity, immediate action shall be taken by the MII such as fine tuning

the applications/systems or enhancing the capacity. SCOT shall oversee such action taken by the MII. The framework for handling actual capacity utilization exceeding 75% of the installed capacity, including situations that would necessitate augmentation of installed capacity, shall be included in the Capacity Planning and Real Time Performance Monitoring Policy of the MII.

For Depositories, if actual capacity utilization of any IT component exceeds 75% of the installed capacity over a period of 15 days on rolling basis, immediate action shall be taken to enhance the capacity..

4.1.1.14. All MIIs shall assess impact of all changes to existing IT systems or introduction of new IT systems/applications/processes on capacity planning and real time system performances.

4.1.1.15. All MIIs shall also appropriately include the capacity planning and real time performance monitoring and alert resolution requirements in the service level agreement (SLA) with the third party vendors, as applicable, to meet the current and future business requirements.

4.1.1.16. All MIIs should have clearly defined 'Capacity Planning and Real Time Performance Monitoring Policy' which shall be approved by their SCOT and Board and would inter-alia cover various requirements of this circular. Further, the policy would require to clearly set out, among others, appropriate system utilization thresholds to provide sufficient time to meet the lead time for procurement of additional resources or take corrective measures during real time. Such policy shall also be reviewed at least on annual basis by the MII.

4.1.2. Considering the above, Stock Exchanges, Clearing Corporations and Depositories are advised to submit their revised guidelines to SEBI on capacity planning and real time performance monitoring of all IT systems after taking approval from SCOT and Governing Board.

5. ADVISORIES RELATED TO TECHNOLOGY

5.1. Advisory on Technology related Investments and Planning by Market Infrastructure Institutions (MIIs) [24]

5.1.1. In order to ensure that technology systems of MIIs keep up with the advancement and sophistication in the field of technology, continuous monitoring of technology infrastructure and systems, along with that of allied processes, is needed for early identification of requirements pertaining to additional investments in technology infrastructure/ systems and technology related human resources.

5.1.2. Accordingly, MIIs are advised to:

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

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

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

5.1.2.4. Review organisational structure and employee strengths across various IT/ technology related departments/verticals. This should include review of outsourcing policies and responsibility mapping of internal staff for such outsourced functions.

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

5.2. Advisory on automation/review of operational processes involving IT systems of Market Infrastructure Institutions (MIIs) [25]

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

[24] SEBI letter dated December 27, 2023
[25] SEBI letter dated April 23, 2024

production release of components, become critical in eliminating technology / operational risk.

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

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

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

5.2.2.3. Ensure that all activities/processes related to or impacting system configuration, for clauses 5.2.2.1 and 5.2.2.2 above, are carried out or overseen by employee(s) of MII competent to understand the operational implications of such technical activities.

5.3. **Process for freezing/un-freezing of accounts/holdings pursuant to issuance of orders of SEBI/ Securities Appellate Tribunal(SAT)/ Supreme Court of India/ other courts[26]**

5.3.1. At present, orders issued by SEBI and/or Hon'ble SAT/Supreme Court of India/other courts (hereinafter referred to as tribunal/court) are intimated to Market Infrastructure Institutions (MIIs), Mutual Funds(MFs) and Registrar and Transfer Agents (RTAs) for taking consequent actions by the concerned Department of SEBI.

5.3.2. In order to streamline and expedite the said process of taking consequent actions pursuant to issuance of orders by SEBI and/or tribunal/court, directing freezing/ un-freezing of accounts/holdings, it has been decided to introduce a new automated mechanism, which would be monitored by a Centralized Coordination Cell of SEBI. The salient features of the new mechanism are as follows: -

5.3.2.1. An automated process would be set up for sending intimations by SEBI to MIIs, MFs and RTAs in a standardized format from the SEBI's Case Management System(CMS) portal in respect of issuance of orders by

[26] SEBI letter dated February 22, 2024

SEBI and/or tribunal/court for freezing/un-freezing of accounts/holdings for seamless implementation of the directions.

5.3.2.2. A Centralized Coordination Cell under the Enforcement Department-1 (EFD-1) of SEBI has been formed to monitor/ensure timely compliance with directions for freezing/un-freezing of accounts/holdings in a time bound manner. The cell will undertake the necessary co-ordination with MIIs, MFs, RTAs and/or the concerned department of SEBI for timely implementation of the directions.

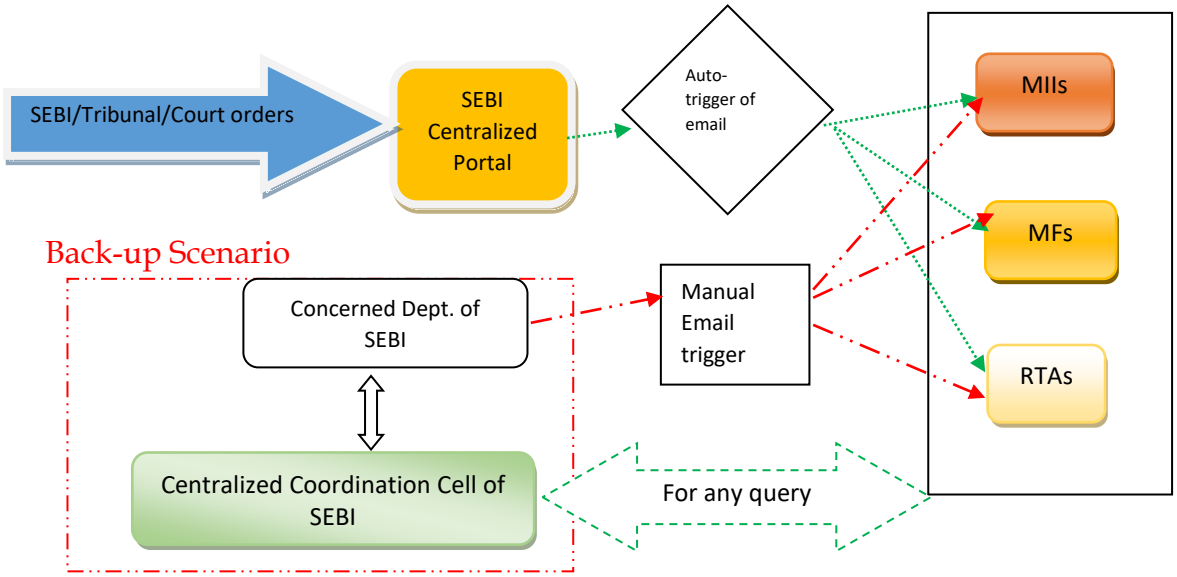
5.3.2.3. In order to ensure that the consequent actions pursuant to issuance of orders by SEBI and/or tribunal/court are acted upon on an immediate basis, the intimations regarding the orders of SEBI and/or tribunal/court directing freezing/ un-freezing of accounts/holdings, would be sent to the generic email IDs of MIIs, MFs and RTAs.

5.3.2.4. MIIs, MFs and RTAs shall establish clear ownership of their dedicated generic email ID at all times and ensure that there is due diligence at their end to ensure compliance with orders of SEBI and/or tribunal/court in a time bound manner.

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

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

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



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

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

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

5.4. Segregation of IT Infrastructure and activities between Stock Exchanges and Clearing Corporations[27]

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

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

5.4.1.2. With respect to the common infrastructure shared by a Stock Exchange (SE) and a Clearing Corporation (CC) with logical segregation, if there is a vulnerability reported in the VAPT audit of SE (or CC), the same should be shared with CC (or SE) and the closure of such vulnerability should also be informed.

5.4.1.3. There should be a logical separation between the persons responsible for handling the networks of SE and CC. Further, for the same kind of activity by SE and CC, there should be a maker-checker mechanism for each other.

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

[27] Emails dated July 29, 2025 and June 21, 2024 on "Segregation of IT Infrastructure and activities between stock exchanges and clearing corporations"

5.4.2. Stock Exchanges and Clearing Corporations are hereby advised to ensure segregation of infrastructure.

6. **REFERENCE: List of Circulars**

1. *SEBI Email dated November 11, 2017 captioned Bolstering Cyber Resiliency*
2. *Circular No. CIR/MRD/CSC/148/2018 dated December 07, 2018*
3. *Circular No. SEBI/HO/MRD/DoP1/CIR/P/2019/24 dated January 31, 2019*
4. *SEBI Letter SEBI/HO/MRD/CSC/OW/P/2019/22202/1 dated August 28, 2019*
5. *Circular No. SEBI/HO/MRD2/DCAP/CIR/P/227 November 06, 2020*
6. *Circular No. SEBI/HO/MRD1/DTCS/CIR/P/2021/33 March 22, 2021*
7. *Circular No. SEBI/HO/MRD1/DTCS/CIR/P/2021/590 dated July 05, 2021*
8. *SEBI Email dated January 31, 2022 w.r.t measures to strengthen tracking and reporting of delay in pay-in/pay-out for rolling settlement*
9. *Circular No. SEBI/HO/MRD1/MRD1_DTCS/P/CIR/2022/58 dated May 02, 2022*
10. *SEBI Email dated September 12, 2022 w.r.t advisory on Security Patch Management Policy*
11. *SEBI Email dated December 28, 2022 w.r.t advisory on Cyber Audit and VAPT*
12. *Circular No. SEBI/HO/MRD-TPD-1/CIR/P/2023/7 dated January 09, 2023*
13. *Circular No. SEBI/HO/MRD/TPD/P/CIR/2023/65 dated May 05, 2023*
14. *Circular No. SEBI/HO/MRD/TPD/P/CIR/2023/192 dated December 20, 2023*
15. *SEBI letter dated December 27, 2023 w.r.t advisory on Technology related Investments and Planning by MIIs*
16. *SEBI letter dated February 22, 2024 w.r.t Process for freezing/un-freezing of accounts/holdings pursuant to issuance of orders of SEBI/ Securities Appellate Tribunal(SAT)/ Supreme Court of India/ other courts*
17. *SEBI letter dated April 23, 2024 w.r.t advisory on automation/review of operational processes involving IT systems of Market Infrastructure Institutions (MIIs)*
18. *Circular No. SEBI/HO/MRD/MRD-PoD-1/P/CIR/2024/62 dated May 27, 2024*
19. *Circular No. SEBI/HO/MRD/TPD-1/P/CIR/2024/119 dated September 12, 2024*
20. *Circular No. SEBI/HO/MRD/TPD-1/P/CIR/2024/124 dated September 20, 2024*
21. *Circular No. SEBI/HO/MRD/TPD/P/CIR/2024/167 dated November 28, 2024*
22. *Circular No. SEBI/HO/MRD/TPD/CIR/P/2024/171 dated December 10, 2024*
23. *Circular No. SEBI/HO/MRD/TPD/CIR/P/2025/08 dated January 28, 2025*
24. *Circular No. SEBI/HO/MRD/TPD/CIR/P/2025/50 dated April 04,2025*
25. *Email dated April 25, 2025 of SEBI on "Advisory for reporting of technical glitches"*
26. *Email dated July 29, 2025 of SEBI on "Action points arising out of meeting of TAC held on March 27, 2025 w.r.t system and network audit reports submitted by MIIs"*
27. *Emails dated July 29, 2025 and June 21, 2024 on "Segregation of IT Infrastructure and activities between stock exchanges and clearing corporations"*
28. *Circular No. HO/47/13/14(1)2026-MRD-TPD1/I/4755/2026 dated February 11, 2026*

Annexure I

System and Network Audit Framework

Audit Process

1. For the System and Network Audit, the following broad areas shall be considered in order to ensure that the audit is comprehensive and effective:

   a. The Audit shall be conducted according to the Norms, Terms of Reference (TOR) and Guidelines issued by SEBI.

   b. The Governing Board of the Market Infrastructure Institution (MII) shall appoint the Auditors based on the prescribed Auditor Selection Norms and TOR.

   c. An Auditor can perform audit for maximum 3 successive years. However, such auditor shall be eligible for re-appointment after a cooling-off period of two years.

   d. Further, during the cooling-off period, the incoming auditor may not include:

      (i) Any firm that has common partner(s) with the outgoing audit firm; and

      (ii) Any associate/ affiliate firm(s) of the outgoing audit firm which are under the same network of audit firms wherein the term "same network" includes the firms operating or functioning, hitherto or in future, under the same brand name, trade name or common control.

   e. The number of years an auditor has performed an audit prior to this circular shall also be considered in order to determine its eligibility in terms of sub-clause c above.

   f. The scope of the Audit may be broadened by the Auditor to inter-alia incorporate any new developments that may arise due to issuance of circulars/ directions/ advice / guidance by SEBI from time to time. In this regard, MIIs shall prepare a detailed SOP on checking of various compliance requirements for the purpose of audit. While framing this SOP, MIIs shall adhere to the guidelines prescribed in this Circular as well as directions/ advice / guidance or otherwise issued by SEBI from time to time.

   g. The audit shall be conducted once in a financial year and period of audit shall be 12 months. However, for the MIIs, whose systems have been identified as "protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC), the audit shall be conducted on a half yearly basis and audit period shall be of 6 months. Further, the audit shall be completed, and the report shall be submitted to SEBI within 3 months from the end of audit period.

h. In the Audit report, the Auditor shall include its comments on whether the areas covered in the Audit are in compliance with the circulars/ directions/ advices issued by SEBI, each of the major areas mentioned in TOR, internal policy of the MII, etc. Further, the audit report shall also include specific non-compliances (NCs), observations for minor deviations and suggestions for improvement for each section based upon the best industry practices. The audit report shall take previous audit reports into consideration and cover any open items therein. The auditor should indicate if a follow-on audit is required to review the status of NCs.

i. For each of the NCs/ observations and suggestions made by the Auditor, specific corrective action as deemed fit may be taken by the MII at the earliest. The management of the MII shall provide its comments on the NCs, observations and suggestions made by the Auditor, corrective actions taken or proposed to be taken along with time-line for such corrective actions.

j. The follow-on audit should be completed by next quarter of submission of the audit report. After the follow-on audit, the MII shall submit a report to SEBI within 1 month from the date of completion of the follow-on audit. The report shall include updated Issue-Log to indicate the corrective actions taken and specific comments of the Auditor on the NCs and the corrective actions. The next system audit report shall cover in detail the points not covered in follow on audit, if any.

k. In cases wherein follow-on audit is not required, the MII shall submit an Action Taken Report (ATR) to the Auditor. After verification of the ATR by the Auditor, the MII shall submit a report to SEBI within 1 month from the date of completion of verification by the Auditor. The report shall include updated Issue-Log to indicate the corrective actions taken and specific comments of the auditor on the ATR.

l. The overall timeline from the last date of the audit period till completion of final compliance by MII, including follow-on audit, if any, should not exceed one year/6 months (as applicable). In exceptional cases, if MII is of the view that compliance with certain observations may extend beyond said period, then the concerned MII shall seek specific approval from the Governing Board.

Auditor Selection Norms

2. MII shall ensure compliance with the following norms while appointing Auditor:

a. The auditor must have minimum 3 years of demonstrable experience in IT audit of securities market participants e.g. stock exchanges, clearing corporations, depositories, intermediaries, etc. and/ or financial services sector i.e. banking, insurance, Fin-tech etc.

b. The team performing system and network audit must have experience in / direct access to experienced resources in the areas covered under TOR. It is recommended that resources deployed by the Auditor for the purpose of system and network audit shall have relevant industry recognized certifications e.g. CISA (Certified Information Systems Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, GSNA (GIAC Systems and Network Auditor), CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium, commonly known as (ISC).

c. The Auditor shall have experience in working on Network Audit/IT audit/governance/IT service management frameworks and processes conforming to industry leading practices like CobiT/ ISO 27001 and beyond.

d. The Auditor should have the capability to undertake forensic audit and undertake such audit as part of system and network audit, if required.

e. The Auditor must not have any conflict of interest in conducting fair, objective and independent audit of the exchange / depository/ clearing corporation. It should not have been engaged over the last three years in any consulting engagement with any departments / units of the entity being audited.

f. The Auditor should not have any cases pending against it, which point to its incompetence and/or unsuitability to perform the audit task.

g. The proposed audit agency must be empanelled with CERT-In.

h. In order to avoid development of conflict of interest, adequate cooling-off period shall be ensured in case of rotation of auditors for different kinds of audits of MIIs.

i. Any criteria, in addition to the aforesaid criteria, that the MII may deem fit for the purpose of selection of Auditor.

Audit Report Guidelines

3. The auditor shall certify that entire network architecture, connectivity (including co-lo facility) and its linkage to the trading infrastructure are in conformity with SEBI's regulatory framework to provide fair equitable, transparent and non-discriminatory treatment to all the market participants.
4. The report should also include tabulated data to show NCs / observations for each of the major areas in the TOR.
5. The audit report to include point-wise compliance of areas prescribed in Terms of Reference (TOR) and areas emanating from relevant SEBI circulars/directions/advices along with any accompanying evidence.
6. Evidences should be specified in the audit report while reporting/ closing an issue.
7. A detailed report with regard to the system and network audit shall be submitted to SEBI. The report shall include an Executive Summary as per the following format:

Issue Log Column Heading	**Description**	**Responsibility**
Major Area	Comprehensive identification of major areas in compliance with various SEBI circulars / norms and internal policies of MII	Auditor/Auditee
Point wise Compliance	Point-wise list of areas/relevant clauses in TOR against which compliance is being audited (in tabular format)	Auditor
Description of Finding/ Observation	Describe the findings in sufficient detail, referencing any accompanying evidence (e.g. procedure manual, interview notes, reports etc.)	Auditor
Reference	Reference to the section in detailed report – where full background information about the findings are available	Auditor
Process/ Unit	Process or unit where the audit is conducted and the finding pertains to	Auditor
Category of Findings	Major/Minor Non-compliance, Observation, Suggestion etc.	Auditor
Audited By	Which Auditor covered the findings	Auditor
Root Cause Analysis	A detailed analysis on the cause of the Non-compliance	Auditee

Remediation	The action (to be) taken to correct the Non-compliance	Auditee
Target Completion Date for Remedial Action	The date by which remedial action must be/will be completed	Auditor/Auditee
Status	Status of finding on reporting date (open/close)	Auditor/Auditee
Verified By	Auditing personnel (upon verification that finding can be closed)	Auditor
Closing Date	Date when finding is verified and can be closed	Auditor

Annexure II

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

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

2. **IT environment**
   2.1. Organization details
      a. Name
      b. Address
      c. IT team size (in house- employees)
      d. IT team size (vendors)
   2.2. IT and network set up and usage
      a. PDC, DRS, NS and Regional/ Branch offices (location, owned/ outsourced)
      b. Connectivity amongst PDC, NS and DRS
      c. IT infrastructure / applications pertaining to the activities done as a MII
      d. System Architecture
      e. Network Architecture
      f. Telecommunication network

3. **IT Governance**
   3.1. Whether IT Governance framework exists to include the following:
      a. IT organization structure including roles and responsibilities of key IT personnel;
      b. IT governance processes including policy making, implementation and monitoring to ensure that the governance principles are followed;
   3.2. IT policies and procedures
      a. Whether the organization has a defined and documented IT policy? If yes, is it approved by the Governing Board (GB)?
      b. Is the current System Architecture including infrastructure, network and application components describing system linkages and dependencies, documented?
      c. Whether defined and documented Standard Operating Procedures (SOPs) for the following processes are in place?
         i. IT Assets Acquisition
         ii. Access Management

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

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

4. **Business Controls**

4.1. General Controls for Data Centre Facilities

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

4.2. Software change control

a. Whether pre-implementation review of application controls (including controls over change management) was undertaken?

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

4.3. Data Communication/ Network Controls

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

4.4. Security Controls

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

4.5. Access Policy and Controls

a. Defined and documented policies and procedures for managing access to applications and infrastructure – PDC, DRS, NS, branches (including network, operating systems and database) and approved by relevant authority

b. Review of access logs
c. Access rights and roles review procedures for all systems
d. Segregation of Duties (SOD) matrix describing key roles
e. Risk acceptance for violation of SOPs and alternate mechanism put in place
f. Privileged access to system and record of logs,
g. Periodic monitoring of access rights for privileged users
h. Authentication mechanisms used for access to systems including use of passwords, One Time Passwords (OTP), Single Sign on, etc.
i. Any other controls, as deemed fit, by the MII

4.6. Electronic Document Controls
4.7. General Access Controls
4.8. Performance Audit
a. Comparison of changes in transaction volumes since previous audit
b. Review of systems (hardware, software, network) performance over the period
c. Review of the current volumes against the last performance test and against the current system utilization
4.9. Business Continuity / Disaster Recovery Facilities
a. a. Business Continuity Planning (BCP) manual, including Business Impact Analysis (BIA), Risk Assessment and Disaster Recovery (DR) process, Roles and responsibilities of Incident Response Team (IRT) /Crisis Management Team (CMT), employees, support/outsourced staff
b. Implementation of policies
c. Back-up procedures and recovery mechanism using back-ups
d. Storage of Back-up (Remote site, DRS etc.)
e. Redundancy – Equipment, Network, Site etc.
f. DRS installation and Drills - Management statement on targeted resumption capability (in terms of time required & extent of loss of data)
g. Evidence of achieving the set targets during the DR drills in event of various disaster scenarios
h. Debrief / review of any actual event when the DR/BCP was invoked during the year
i. User awareness and training
j. Is Recovery Time Objective (RTO) /Recovery Point Objective (RPO) during BIA documented?
k. Is annual review of BCP-DR or in case of major change in business/ infrastructure undertaken?
l. Is quarterly review regarding implementation of BCP policy done by Standing Committee of Technology (SCOT) of the MII?

m. Testing of BCP-DR plan through appropriate strategies including simulations, DR drills, system recovery, etc.
n. Is the recordkeeping of quarterly DR drills, live trading sessions from DRS being maintained?
o. Is BCP-DR policy document prepared and implemented in line with SEBI circular on BCP and DR of MII?

4.10. IT/Network Support & IT Asset Management

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

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

6. **Human Resources Management**

6.1. Screening of Employee, Third party vendors / contractors

6.2. Onboarding

6.3. Offboarding

6.4. Consequence Management (Incident / Breach of policies)

6.5. Awareness and Trainings

6.6. Non-Disclosure Agreements (NDAs) and confidentiality agreement

7. **Network Audit**

7.1. The audit shall cover entire network infrastructure which shall inter-alia includes physical verification and tracing of the connectivity paths, server configuration, physical checking wire to wire connectivity and configurations of computer networking devices etc.

7.2. The audit shall require tracing of the connectivity and network diagram based on the physical audit.

7.3. The audit shall cover the link, the path, device-level redundancy, no single-

point failures, high availability, and fault tolerance aspects in the network.

7.4. The audit shall cover entire network that is used to connect members to the MIIs (POP, MPLS, VSAT, COLO, etc.)

7.5. The audit shall cover applications, internal networks, servers, etc. of the MIIs/offered by the MIIs to its members that are used for trading, risk management, clearing and settlement etc.

7.6. Network performance and design

7.7. Network Security implementation

7.8. Network health monitoring and alert system

7.9. Log management process

7.10. Service level definition for vendors/Service level management

7.11. Governance process for network service delivery by vendors

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

9. **IT Vendor Selection and Management**

9.1. Identification of eligible vendors

9.2. Dissemination process of Request for Proposal (RFP)

9.3. Definition of criteria of evaluation

9.4. Process of competitive analysis

9.5. Approach for selection

9.6. Escrow arrangement for keeping source code

10. **E-Mail system**

10.1. Existence of policy for the acceptable use of electronic mail

10.2. Regulations governing file transfer and exchange of messages with external parties

10.3. Rules based on which e-mail addresses are assigned

10.4. Storage, backup and retrieval

11. **Redressal of Technological Complaints**

    11.1. Ageing analysis of technology complaints

    11.2. Whether all complaints received are brought to their logical conclusion?

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

    12.1. Electronic Waste Disposal

    12.2. Observation(s) based on previous Audit Report(s)

    12.3. In case of Commodity Derivatives segment, Type I brokers may be exempted from system audit and the development of NEAT / BOLT /Stock Exchange provided terminals and provisions relating to Type I Brokers shall be included in the scope of System Audit of stock exchanges with Commodity Derivatives segment.

    12.4. Any other specific area(s) that may be informed by SEBI.

Annexure III

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

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

Annexure IV

Exception Observation Reporting Format

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

Name of the MII: _____

Name of the Auditor: _____

System and Network Audit Report Date: _____

Table 1: For preliminary audit

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

Description of relevant Table heads

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

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

Rating	Description
HIGH	Represents weakness in control with respect to threat(s) that is /are sufficiently capable and impacts asset (s) leading to regulatory non-compliance, significant financial, operational and reputational loss. These observations need to be addressed with utmost priority.
MEDIUM	Represents weakness in control with respect to threat(s) that is /are sufficiently capable and impacts asset (s) leading to exposure in terms of financial, operational and reputational loss. These observations need to be addressed in reasonable timeframe.
LOW	Represents weaknesses in control, which in combination with other weakness can develop into an exposure. Suggested improvements for situations not immediately/directly affecting controls.

5. **Audit TOR clause –** The TOR clause corresponding to this observation
6. **Root Cause analysis –** A detailed analysis on the cause of the non-conformity.
7. **Impact Analysis –** An analysis of the likely impact on the operations/ activity of the organization
8. **Corrective Action –** The action taken to correct the non-conformity

Table 2: For follow on/ follow up system and Network audit

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

Description of relevant Table heads

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

****

Annexure IVA

1. Background: -

2. Details of Auditee:-

Auditee Name	
Auditee Address	
Contact Information	
Date of agreement between MII and auditor	

3. Details of Audit Team Members: -

Auditor Name	
Auditor address	
Contact information	
Location of audit	
Audit team members and details of qualifications	

4. Information about audit: -

Audit Period	
Date of start of audit	
Date of end of audit	
Date of audit report	

5. Overview of IT environment of MII (including any major projects/positive development undertaken during audit period)

6. Scope of audit/Terms of reference (as agreed between the auditee and auditor), including the standard/specific scope for audit as defined by SEBI: -

    a. List of SEBI Circulars and Advisories covered during the audit: -

    b. List of various rule based regulatory requirements defined by SEBI related to IT resilience/Technology Risk Management (TRM), covered during the audit: -

    For instance, Disaster Recovery (DR) drills on quarterly basis, Live trading sessions from DR site, Review of BCP-DR policy, Review of capacity planning as per projected peak load and other relevant factors, Stress testing of existing load scenarios on quarterly basis, Review of performance monitoring and alert

systems on quarterly basis, Review of Capacity Planning and Real Time Performance Monitoring Policy, Mock session of SaaS-RMS on quarterly basis etc.

c. List of technical glitches covered during the audit: -

d. List of all IT/network infrastructure (including IT systems/applications/database management systems of Primary Data Center (PDC), Disaster Recovery Site (DRS), Near Site, Co-lo facility) covered under audit: -

e. Geographical locations covered under audit (PDC/DRS/Near Site etc.): -

f. Name of audit tools used during audit, if any: -

g. Any other specific item(s): -

7. Methodology /Audit approach (audit subject identification, pre-audit planning, data gathering methodology, sampling methodology etc. followed): -

8. Executive Summary of findings (including identification tests, tools used and results of tests performed): -

S.No	Number of observations	Risk rating			Any other comments
		High	Medium	Low	

9. Control-wise compliance status of various SEBI Circulars /Advisories related to technology: -

S. No.	Date of SEBI circular/ direction / advice, etc.	Requirements specified by SEBI in brief	Mechanism put in place by MIIs	Compliance status ('Yes' / 'No')	Details of Non Compliance with SEBI circulars/ directions, etc.(applicable only in case of non-compliance)	*List of documentary evidence including physical verification	**Unique Observation ID (in case of non-compliance /observation found during audit)	Associated risks in case Compliance status is 'No'	Path of file system where details of supporting annexures of non-

									compliances are placed

*Explicit reference to the key auditee organisational documents (by date or version) including policy and procedure documents

**Unique ID shall be assigned to each unique observation found during audit and its format shall be "Name of MII-SNFYYYY". The description of the same is mentioned below: -

S.NO	Heading	Interpretation
1	Name of MII	Name of MII shall be written in short form such as NSE/BSE/NCL/ICCL/MSEI/NSDL/CDSL/MCX/MCXCCL /NCCL/NCDEX
2	S	S represents observation found in System and Network audit
3	N	N represents i^{th} observation found during particular audit period i.e. serial number of unique observation i.e. 1,2……n.
4	F	F represents frequency of audit i.e. value of F=0 in case of audit is being done for full financial year, F=1 in case of audit is being done for first half of any financial year, F=2 in case of audit is being done for second half of any financial year.
5	YYYY	YYYY represents the financial year for which audit is being carried out by auditor

For instance, Unique ID NSE-S122324 represents the observation serial number 1 found in second half of FY 2023-24 of System and Network audit of NSE, Similarly, Unique ID CDSL-S212425 represents the observation serial number 2 found in first half of FY 2024-25 of System and Network audit of CDSL. Unique ID ICCL-S302425 represents the observation serial number 3 found in audit period of FY 2024-25 of System and Network audit of ICCL.

10. Compliance status of various rule based regulatory requirements related to IT resilience mandated by SEBI: -

S.No.	Name of regulatory report /requirements	Brief about regulatory requirements	Compliance status ('Yes'/ 'No')	List of documentary evidence including physical inspection	**Unique Observation ID(in case of non-compliance found during audit)	Associated risks in case compliance status is 'No'	Comments on comprehensiveness of exercise
1	DR drills						
2	Live trading sessions						
3	Stress testing of existing load scenarios						
4	Mock session of SaaS-RMS (applicable for NCL and ICCL)						
5	Review of BCP-DR policy						
6	Review of Capacity Planning and Real Time Performance Monitoring Policy						
7	Review of performance monitoring and alert systems						
8	Review of Capacity						

S.No.	Name of regulatory report /requirements	Brief about regulatory requirements	Compliance status ('Yes'/ 'No')	List of documentary evidence including physical inspection	**Unique Observation ID(in case of non-compliance found during audit)	Associated risks in case compliance status is 'No'	Comments on comprehensiveness of exercise
	planning as per projected peak load and other relevant factors						

**Similar format mentioned in point number 9 above

11. Compliance status of corrective action taken for technical glitches occurred at MIIs during audit period: -

S.No.	Date of technical glitch	Brief about incident	Corrective action suggested by SCOT/SEBI/MIIs	Compliance status of corrective action to be taken by concerned MII('Yes'/ 'No')	List of documentary evidence including physical inspection	**Unique Observation ID(in case of non-compliance found during audit)	Associated risks in case compliance status is 'No'	Any other comments by auditor

**Similar format mentioned in point number 9 above

12. Open observation reporting format as per Annexure IV of this Circular for MIIs. It may be noted that the abovementioned Unique observation ID shall be quoted in the open observation reporting format.

13. List of observations pending for closure which are pertaining to previous audits: -

S. No	Unique observatio	Name and	Relevant	Details of open	Open observati	Reasons for	Comments of

.	n ID assigned by auditor in previous audits (may be left blank for observations found before the date of issuance of this Circular)	date of SEBI Circular	Clause of SEBI Circular	observation	on pertaining to which audit period	pending for closure-comments of management	auditor including risk associated with non-closure of observation

14. Limitations, if any

15. Any other relevant comments by the auditor

16. Conclusion

Annexure V

1. In order to ensure compliance with the guidelines for Business Continuity Plan (BCP) and Disaster Recovery (DR), prescribed at Para 2.1 of this Circular for MIIs, LPCC is permitted to have arrangements with any of the existing Clearing Corporations who are in compliance with the existing regulatory BCP/DR requirements. However, for any issues / disputes arising on account of such arrangement, the LPCC shall be liable. Hence, the LPCC shall incorporate necessary provision into its agreement with the service providers for its BCP/DR arrangement with them.

2. Similarly, in order to ensure compliance with the requirements relating to the prescribed Cyber Security and Cyber Resilience framework at Para 10.1 and 10.6 of this Chapter of Master Circular for Stock Exchanges and Clearing Corporations, LPCC is permitted to have outsourcing arrangements for cyber security with any of the existing Clearing Corporations for the purposes of Cyber Security. For any issues / disputes arising on account of such arrangement, LPCC would be liable.

Annexure VI

Standard Operating Procedure (SOP) for handling of technical glitches

Definition of "Technical Glitch"

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

Reporting Requirements

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

Sl. No.	Disruption	Reporting
1.	No business disruption	• Standing Committee on Technology (SCOT) of MII • Governing Board of MII
2.	Business disruption	• SCOT of MII • Governing Board of MII • SEBI

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

2.1. With regard to incidents resulting in business disruption, the following shall be submitted by the MIIs to SEBI:

(i) Information of technical glitch on immediate basis but not later than 2 hours from the time of occurrence of the glitch; provided that glitches of the nature of a disaster- as defined above in Clause 2.1.2.3 - shall be reported immediately upon declaration of disaster.

(ii) Preliminary report within 24 hours of the occurrence of the glitch.

(iii) Comprehensive Root Cause Analysis (RCA) report and corrective action taken to address the technical glitch within 21 days of the incident. Such report shall be submitted to SEBI, after placing the same before the Standing Committee on Technology and the Governing Board of the MII and confirming compliance with their observations.

(iv) RCA submitted by the MIIs should inter-alia include exact cause of the technical glitch (including root cause from vendor(s), if applicable), exact duration of the technical glitch, chronology of events, list of business

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

2.2. The preliminary and RCA report of technical glitch shall be shared by the MII with SEBI through a dedicated web based portal of SEBI viz. iSPOT (Integrated SEBI Portal for Technical Glitches).

2.3. SEBI on identification of the Technical Glitch resulting into Financial Disincentive to the MIIs, or upon receipt of the information of any such instance shall provide an opportunity to the concerned MIIs to make their submissions in respect of the facts of the case.

2.4. MIIs shall carry out internal examination pertaining to occurrence of technical glitches to ascertain individual accountability and take appropriate action including suitable recording and reckoning in the performance appraisal of those individuals. SEBI would retain the right to initiate enforcement action against the individuals at the MII, if there is sufficient ground to do so.

Placing before Technical Advisory Committee (TAC)

3. With regard to the incidents wherein business is disrupted, the RCA and corrective action taken, as submitted by the MII, shall be placed before TAC of SEBI. TAC/ SEBI, if it so desires, may seek additional information/ clarification from the MII regarding the technical glitch.

4. In case TAC finds the actions taken by the MII as inadequate, then, based on the recommendations of TAC, the MII shall be required to address the technical glitch by taking appropriate corrective actions, within the timeline specified by TAC/SEBI. While deciding such timeline, criticality of the malfunction and/or the services/ applications affected by the same shall also be taken into consideration.

Annexure VII

"Financial Disincentive" structure with regard to handling of technical glitches

Failure to timely submit RCA

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

Failure to timely address technical glitch

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

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

Failure to declare disaster within stipulated timelines

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

S No.	Delay in declaration of disaster beyond abovementioned timeline specified by SEBI	Financial disincentive Equivalent (Rs.)
i.	Financial disincentive on MII	10% of average of standalone net profit for previous two financial years or Rs. 2 cr., whichever is higher.

Failure to restore operations within Recovery Time Objective (RTO)

4. In the event of a disaster, if an MII fails to restore its operations within the RTO prescribed by SEBI, i.e. to restore operations of 'Critical Systems' including from

Disaster Recovery Site within 45 minutes of declaration of Disaster, the following "financial disincentive" shall be paid:

S No.	Failure to restore operations within the RTO prescribed by SEBI	Financial disincentive Equivalent (Rs.)
i.	Financial disincentive on MII	10% of average of standalone net profit for previous two financial years or Rs. 2 cr., whichever is higher.

"Financial disincentive" under Clause 3 and Clause 4 above, in relation to the same disaster, shall be paid only once either under Clause 3 or Clause 4.

5. Further, if an MII fails to restore operations of Critical Systems including from Disaster Recovery Site within three hours from the occurrence of the disaster, the following additional "financial disincentive" (over and above S No 3 or 4 above) shall be paid:

S No.	Failure to Restore operations of Critical systems beyond abovementioned timeline	Financial disincentive Equivalent (Rs.)
i.	Financial disincentive on MII	10% of average of standalone net profit for previous two financial years or Rs. 2 cr., whichever is higher.

Failure to restore normalcy in cases of business disruption, not being in the nature of a Disaster

6. In the event of any business disruption, which is not required to be declared as "Disaster", if an MII fails to restore normalcy of operations within 75 minutes of the incident, the following slab wise "financial disincentive" shall be paid by the MII:

S No.	Failure to Restore normalcy within	Financial disincentive (Rs.)
i.	75 minutes to 3 hours of the incident	Rs. 50 lacs
ii.	Beyond 3 hours of the incident	Rs.1 crore

7. The amount of "financial disincentive" paid as per the above structure shall be credited by MII to the following funds maintained by it:

S No.	Financial Disincentive on MIIs	Credited to Funds

i.	Stock Exchange	Investor Protection Fund (IPF)
ii.	Clearing Corporation	Core Settlement Guarantee Fund (Core SGF)
iii.	Depositories	Investor Protection Fund (IPF)

8. Further, the MII shall submit a compliance report within 90 days of occurrence of disaster/ business disruption to SEBI providing details of payment of "financial disincentives" including computation of "financial disincentives" as per the SOP and the date when the amount was credited to the aforementioned funds.
9. MIIs shall disclose on their websites (and in their respective annual reports), the details of financial disincentive paid by them on account of technical glitches. Further, listed MIIs shall make appropriate disclosures required in terms of SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 regarding any financial disincentive imposed by SEBI on account of technical glitch.
10. The financial disincentives automatically triggered under predefined circumstances as stated in clauses 1, 2, 3, 4, 5, 6 above shall be paid by the MIIs. However, these financial disincentives shall be without prejudice to any action as may be initiated by SEBI.

****

Annexure VIII

1. Level of support definitions for outsourcing/in-house are as follows:

1.1. Security Analyst Level 1 (L1): This function may be mostly outsourced

(a) Monitoring SIEM Solution console for identifying the security events generated by the log sources integrated with SIEM tools.
(b) Identification of security events that are false +ve before qualifying event as an incident.
(c) Identify the exceptions which are identified as an event (e.g. VA scanning performed by SEBI appointed 3rd party which may be identified as port scanning attack).
(d) Perform first level event analysis before qualifying the incidents.
(e) Qualifying the event as an incident using Knowledgebase.
(f) Escalating exceptions & Events to L2 level.
(g) Log Incident tickets in service management tool and assign it to the respective team.
(h) Follow-up for the closure of the incident tickets generated.

1.2. Security Analyst Level 2 (L2): Combination of Outsource / In-House

(a) Exception Analysis.
(b) Analysis of extended events.
(c) Confirmation of False +ve & update Knowledge Base.
(d) Qualify Incident & provide mitigation suggestions.
(e) Escalate incident to next level.
(f) Update /configuration correlation rules after approval.

1.3. Security Analyst Level 3 (L3): Combination of Outsource / In-House

(a) Analysis of escalated Incidents.
(b) Define correlation rules.
(c) Analysis of impact on SIEM over all correlation rules and operations for the correlation rules suggested by Level 2 Analyst.
(d) Approve correlation rules after the impact analysis.
(e) Perform impact analysis before deployment of correlation rules.
(f) Perform impact analysis for update and upgrade of SIEM & Advance security solutions components.
(g) Define Mitigation suggestions for newly identified incidents.

(h) Approve the reports before sharing with others.

1.4. SOC Manager (L4) : In-house

(a) Lead and manage Security Operations Centre.
(b) Provide strategic directions to SOC team and organization for security posture improvements.
(c) To identify key contacts for incident escalation and change management activities.
(d) Ensure compliance to SLA.
(e) Ensure process adherence and process improvisation to achieve operational objectives.
(f) Revise and develop processes to strengthen the current Security Operations.
(g) Responsible for team and vendor management.
(h) Responsible for overall use of resources and initiation of corrective action where required for Security Operations Center.
(i) Escalate to the other IT Infra. Management teams or application maintenance teams, as necessary.
(j) Overall responsibility for delivery of in scope activities as a part of this engagement.
(k) Point of contact for problem escalation and reporting.

1.5. Security Subject Matter Expert for Security technologies: In-house with reliance on external expertise

(a) Subject Matter Expert (SME) for SIEM and Advance security solutions.
(b) Assist you with troubleshooting steps to be performed by you in order to re-establish connectivity between the SIEM System and SEBI's locations.
(c) Provide software-level management for the SIEM System components;
(d) Verify data collection and log continuity;
(e) Manage user access including user and group permissions updates;
(f) Review application performance, capacity, and availability make recommendations as appropriate;
(g) Review SIEM System disk space usage;
(h) Verify time synchronization among SIEM System components;
(i) Perform archival management and retrieval per change

management process;

(j) Provide problem determination / problem source identification for the SIEM System, consisting of creating tickets & tracking progress of Open tickets

(k) Managing tickets to resolution / closure, in accordance with the processes as defined in the Integrated and Transition vendor announcements & manage SIEM System update alerts;

(l) Install application patches and software updates in order to improve performance, or enable additional functionality

Illustrative Training Requirements

Security Analyst Level 1 (L1):

1) SEC401: Security Essentials Bootcamp Style https://www.sans.org/event/cyber-defence-canberra-2018/course/security-essentials-bootcamp-style
2) SEC301: Introduction to Cyber Security https://www.sans.org/course/introduction-cyber-security

Security Analyst Level 2 (L2):

1) SEC542: Web App Penetration Testing and Ethical Hacking https://www.sans.org/event/cyber-defence-canberra-2018/course/web-app- penetration-testing-ethical-hacking
2) SEC566: Implementing and Auditing the Critical Security Controls - In-Depth https://www.sans.org/private-training/course/implementing-auditing-critical-security- controls
3) SEC575: Mobile Device Security and Ethical Hacking https://www.sans.org/private-training/course/mobile-device-security-ethical-hacking

Security Analyst Level 3 (L3):

1) SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling https://www.sans.org/event/cyber-defence-canberra-2018/course/hacker-techniques-exploits-incident-handling
2) FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting https://www.sans.org/event/digital-forensics-summit-2018/course/advanced-incident- response-threat-hunting-training
3) SEC501: Advanced Security Essentials - Enterprise Defender

https://www.sans.org/private-training/course/advanced-security-essentials- enterprise-defender

4) MGT414: SANS Training Program for CISSP® Certification https://www.sans.org/course/sans-plus-s-training-program-cissp-certification-exam

SOC Manager (L4):

1) Cyber Security Specialist http://www.leaderquestonline.com/it-career-training/cybersecurity-specialist/
2) Managing Security Operations: Detection, Response, and Intelligence https://www.sans.org/event/rocky-mountain-2018/course/managing-security-operations-detection-response-and-intelligence
3) SIEM with Tactical Analytics https://www.sans.org/private-training/course/siem-with-tactical-analytics
4) SEC511: Continuous Monitoring and Security Operations https://www.sans.org/course/continuous-monitoring-security-operations
5) SEC599: Defeating Advanced Adversaries - Implementing Kill Chain Defenses https://www.sans.org/course/defeating-advanced-adversaries-kill-chain-defenses

Annexure IX – 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.

Annexure X - Form to report on AI and ML technologies – to be submitted quarterly

S/N	Head	Value
1	Entity SEBI registration number	
2	Registered entity category	
3	Entity name	
4	Entity PAN no.	
5	Application / System name	
6	Date used from	
7	Type of area where AI or ML is used (order execution / Surveillance / compliance / others). In case of others, please specify.	
8	What is the name of the Tool / Technology that is categorized as AI and ML system / Application and submissions are declared vide this response	<free text field>
9	How was the AI or ML project implemented	<Internally / through solution provider / Jointly with a solution provider or third party>
10	Are the key controls and control points in your AI or ML application or systems in accordance with circular(s) of SEBI that mandate/s cyber security control requirements	<free text field>
11	Is the AI / ML system included in the system audit	<Yes / No>
12	Describe the application /system and how it uses AI / ML	<free text field>
13	What safeguards are in place to prevent abnormal behavior of the AI or ML application / System	<free text field>