CDSL/AUD/DP/POLCY/2026/765 **October 30, 2026**

SUBMISSION OF CYBER SECURITY AUDIT REPORT

Depository Participants are advised to refer SEBI Circular No. 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) and subsequent clarification circulars dated December 31, 2024, March 28, 2025, April 30, 2025, August 28, 2025, and Frequently Asked Questions (FAQ) dated June 11, 2025, issued by SEBI.

As per clause no. 4.4. Cyber Audit of the CSCRF circular dated August 20, 2024, Cyber audit shall cover 100% of the critical systems and 25% of non-critical systems chosen on a sample basis for which the rationale of checking it on sample basis (non-critical systems) and the chosen sample size shall be explicitly mentioned in the audit report by auditor. Further, as per clause no. 4.4.1. of the CSCRF circular dated August 20, 2024, REs shall ensure that no audit cycle shall be left unaudited (if any) due to the change in category in the beginning of the financial year. In all such cases, the unaudited period shall be included in the current audit cycle.

For implementing the CSCRF guidelines on Cyber Audit by REs, the following timelines have been prescribed in consultation with SEBI, for conducting & submitting the Cyber Audit Report on a half yearly basis. These timelines apply tor Depository Participants classified as Qualified REs and Mid-size REs/Small-size REs providing Internet-Based Trading (IBT) or Algo Trading facility.

For Qualified REs , Mid-size REs (providing IBT or Algo trading as a Stockbroker), Small-size REs (providing IBT or Algo trading as Stockbroker):

Audit Period	Applicability	Preliminary Audit Report Submission	Action Taken Report (ATR) (If Applicable)
Half-yearly (April 2026 - September 2026)	i. Qualified REs ii. Mid-size RE who provide IBT or Algo Trading Facility iii. Small-size RE who provide IBT or Algo Trading Facility	December 31st ,2026	March 31, 2027

Classification - Internal

Further, many Depository Participants / RE's are holding multiple registrations/licenses with SEBI for services such as Custody, AIF, RA/IA, PMS, Merchant Bankers etc., for which Exchanges/Depository are not reporting authority, hence for the compliance towards standards & guidelines published under SEBI CSCRF circular dated August 20,2024 & subsequent clarification circulars issued by SEBI, Depository Participants / RE's shall categorized themselves as per criteria laid down in the said circulars.

The categorization such determined by Depository Participants/REs shall be reviewed & approved by the entity's Board of Directors/Designated Director, or the Proprietor or Partner or technical advisory committee, as applicable for each financial year. Additionally, during the course of the Cyber Audit under CSCRF, auditors shall verify/validate whether the categorization determined/provided by the Depository Participants (RE) is in accordance with SEBI CSCRF framework.

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

The auditor selection norms and guidelines to be adhered by auditors/REs for conduct of cyber audit as per the provisions of CSCRF has been given in **Annexure A**. The terms of reference for cyber security audit report are mentioned in **Annexure B**.

While selecting/appointing CERT-In empanelled auditing organization/entity, Depository Participants/REs are advised to assess the number of members the auditing organization/entity is currently servicing and the size of their audit team. This evaluation is essential to ascertain that the audit is comprehensive, and the audit team can dedicate adequate time and resources to ensure the integrity and effectiveness of the audit process is not compromised.

CERT-In has published Comprehensive Cyber Security Audit Policy Guidelines, as these guidelines are intended to serve as a reference to empanelled auditing and auditee organizations. Accordingly, to ensure consistent, effective and secure approach to Cyber Security Audits (as prescribed in SEBI circular dated August 28,2025), REs shall follow Comprehensive Cyber Security Audit Policy Guidelines as published by CERT-In from time to time.

Classification - Internal

The Cyber audit shall indicate the scope/perimeter of the coverage of the systems audited in the cyber audit report regarding the compliances checked including areas (but not limited to) computer hardware, business applications, software, cyber governance, linkage with vendor systems.

The formats of Cyber Audit report, Executive Summary, Auditor Declaration, Scope of Audit, Methodology/ Audit approach, Summary of findings, Control-wise compliance status of SEBI CSCRF and Conclusion of Cyber Audit has been enclosed as **Annexure C**.

Presently DPs were required to submit a consolidated report to CDSL to comply with the abovementioned circular. Failure to submit the report within the stipulated timeline shall be treated as non-compliance, and a penalty shall be levied in accordance with **Communiqué *No: CDSL/AUDIT/DP/POLCY/2025/105 dated February 12, 2025.***

The procedure for uploading Cyber Security Audit Report will be communicated separately .

Queries regarding this communiqué may be sent to dpinfosec@cdslindia.com, or you may contact us on our landline numbers: 022-62343576 / 022-62343461.

For and on behalf of
Central Depository Services (India) Limited

sd/-

Urmila Chougule
Senior Manager - Audit, Inspection & Compliance

Classification - Internal

Annexure A

Auditors Selection Norms & Guidelines to Auditors for Cyber Audit

1. Auditor Selection Norms

a. Auditing Organization/Entity must mandatorily be CERT-In empanelled.

b. Auditor of Auditing Organization/Entity must preferably have a minimum of 3 years of experience in IT audit of Banking and Financial services preferably in the Securities Market. E.g. Stock exchanges, clearing houses, depositories, stockbrokers, depository participants, mutual funds, etc. The audit experience should have covered all the major areas mentioned under various cybersecurity frameworks and guidelines issued by SEBI from time to time. Auditing experience of the Cybersecurity Framework under ISO 27001 for an organization will be an added advantage.

c. The Auditor of Auditing Organization/Entity must have experience in/ direct access to experienced resources in the areas covered under CSCRF. It is recommended that resources employed 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)2.

d. The Auditor of Auditing Organization/Entity shall have ISMS/ IT audit/ governance frameworks and processes conforming to leading industry practices like COBIT.

e. The CERT-In empanelled Auditing Organization/Entity can perform a maximum 3 consecutive years audits of the RE. However, such CERT-In empanelled Auditing Organization/Entity shall be eligible for reappointment after a cooling-off period of two years.

f. The Auditor & Auditing Organization/Entity must not have any conflict of interest in conducting fair, objective and independent audit of the REs. It shall not have been engaged over the last two years in any consulting engagement with any departments/ units of the RE being audited.

g. The Auditor & Auditing Organization/Entity may not have any cases pending against its previous auditees, which fall under SEBI's Jurisdiction, which point to its incompetence and/or unsuitability to perform the audit task.

h. The Auditor of Auditing Organization/Entity shall have experience of performing VAPT.

i. The Auditor of Auditing Organization/Entity must compulsorily use only licensed tools.

j. The Auditing Organization/Entity must compulsorily enter into a Non-disclosure Agreement (NDA) with the auditee. Under no circumstances, the data sought during the review or the audit report subsequently should leave the jurisdiction of India.

Classification - Internal

2. Guidelines to Auditors

To conduct the cyber audit as per the provisions of CSCRF, following are the guidelines to be adhered to:

a. RE shall ensure that NDA is signed between the RE and Auditing Organization/Entity prior to initiation of the cyber audit.
b. All audit reports shall be submitted strictly as per the format provided in CSCRF.
c. The coverage of the audit shall be as follows:
    i. REs which have been declared as CIIs by NCIIPC shall follow the guidelines/ circulars issued by NCIIPC for selecting sample size for critical/ non-critical assets.
    ii. Rest of the REs shall take the sample size as mentioned in 'CSCRF Compliance, Audit Report.
    iii. RE shall ensure that 100% of their *critical systems* should get covered under cyber audit. Further, RE shall ensure that for 25% of non-critical systems, sample size and sampling method should be mentioned explicitly in the audit report with the rationale of checking it on sample basis and the chosen sample size.
    iv. As part of audit of the RE, the auditor of Auditing Organization/Entity shall verify, and certify, whether there is a clear delineation/ demarcation of roles and responsibilities between the RE and Hosted service provider (as given in definitions section). The auditor of Auditing Organization/Entity shall also verify, and certify, whether the above-mentioned demarcations of roles and responsibilities have been incorporated in the agreement/ contract signed between the RE and Hosted service provider.
d. The auditors of Auditing Organization/Entity shall also validate the adherence to the timelines as stated in 'Section 4: CSCRF Compliance, Audit Report Submission, and Timeline's of CSCRF.
e. For mandatory TOR points / guidelines, auditor of Auditing Organization/Entity shall verify whether guidelines have been implemented as mentioned in the CSCRF. If there are any variations, auditors shall mention the same with relevant evidence in their report.
f. For TOR points / non-mandatory guidelines, auditors shall verify that whether REs have implemented equivalent controls or higher. If the implemented measures are not lower/ weaker than the stated guidelines, auditors of Auditing Organization/Entity shall mention the same with proper evidence in their report.
g. For standards where no guidelines are mentioned, auditors shall verify that REs have implemented the industry best practices.

Classification - Internal

h. Auditor of Auditing Organization/Entity shall ensure that the evidence are comprehensively stated with the observations made in the report. Auditors shall provide appropriate description of evidence verified for each standard/guideline.

i. The risk-rating category (critical/ high/ medium/ low) shall be presented clearly in the audit observations.

j. Auditor of Auditing Organization/Entity shall compulsorily give their recommendations and suggestions to mitigate critical and high observations made in the report for the consideration of the REs. REs shall examine these recommendations and take it to their respective IT committee for REs for remediation.

k. REs shall securely store the evidence provided by the auditor. These evidences may be scrutinized during regulatory inspections/investigations.

l. Auditor of Auditing Organization/Entity shall verify the closure of previous audit observations and mention the status of the same in the audit report.

m. If any observation is repeated from the previous audit, auditor of Auditing Organization/Entity shall clearly mention them as repeat observation.

n. Auditor's report(s) shall include assessment of identification of assets as critical/ non-critical.

o. Auditor's report(s) shall be accompanied by the auditor's certificate for adhering to the above-mentioned points.

3. Other recommended references:

a. IT Security Auditing Guidelines for REs: **https://www.cert-in.org.in/PDF/guideline_auditee.pdf**

b. Guidelines for CERT-In empanelled Information Security Auditing Organizations: **https://www.cert-in.org.in/PDF/Auditor_Guidelines.pdf .**

c. Comprehensive Cyber Security Audit Policy Guidelines: **https://www.cert-in.org.in/PDF/Comprehensive_Cyber_Security_Audit_Policy_Guidelines.pdf**

Classification - Internal

Annexure B

Terms of Reference (TOR) applicable for Cyber Audit as per CSCRF

TOR Type	Standard of CSCRF	Details
1	**Governance**	
1(a)	GV.RR.S3	Has the RE designated a senior official as Chief Information Security Officer (CISO) whose function would be to assess, identify, and reduce cybersecurity risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the cybersecurity and cyber resilience policy approved by the Board/Partners/Proprietor of the RE? Is the reporting of the CISO directly to the MD & CEO of their organization? Does the CISO possess sufficient qualification and capabilities to carry out his/her responsibilities? Has the RE established a reporting procedure to facilitate communication of cybersecurity incidents/unusual activities to the CISO or to the senior management in a time-bound manner as defined by guidelines/policies/laws/circulars/regulations, etc.? Is the level, grade, and standing of the CISO at least equivalent to CTO/CIO?
1(a)(i)	GV.RR.S3	Has the RE appointed a senior official or management personnel (the 'Designated Officer') responsible for assessing, identifying, and reducing cybersecurity risks; responding to incidents; establishing appropriate standards and controls; and directing the development and implementation of processes and procedures in line with the cybersecurity and cyber resilience policy approved by the Board, Partners, or Proprietor? Has the RE implemented a reporting procedure to communicate cybersecurity incidents/unusual activities to the Designated Officer within a time-bound framework, in compliance with SEBI or GoI guidelines, policies, laws, circulars, or regulations?
1(b)	GV.RR.S4	Has the RE allocated an adequate percentage of the total IT budget to cybersecurity? Has this allocation been mentioned under a separate

Classification - Internal

		budgetary head for monitoring by the Board of Directors or top-level management?
1(b)(i)	GV.RR.S4	Has the RE ensured that adequate resources are allocated and aligned with the cybersecurity risk strategy, roles and responsibilities, and policies? Whether the resources are defined in terms of budgetary allocation, people, and material, and are resourcing requirements revisited regularly based upon progress or shortfalls in the implementation of standards and reflected in the budgetary allocation?
1(c)	GV.RR.S5, GV.RR.S6	Has the RE ensured that every employee hired, irrespective of the department or role, presents a low/no threat to the REs' cybersecurity posture by following the below steps? 1. Conducting due diligence 2. Ensuring employees receive proper security training during onboarding and on a regular basis 3. Following employment screening procedures, employment policies and agreements, employment termination procedures, etc.?
1(d)	GV.RR.S6	Has the RE signed a confidentiality and integrity agreement with third-party service providers and conducted due diligence of all third-party service providers accessing their IT systems?
1(e)(i)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Has the RE formulated a comprehensive Cybersecurity and Cyber Resilience policy document encompassing CSCRF as part of the operational risk management framework to manage risks to systems, networks and databases from cyber-attacks and threats,?
1(e)(ii)	GV.PO.S1, GV.PO.S2, GV.PO.S5	In case of deviations from the suggested framework, whether reasons for such deviations, technical or otherwise, are provided in the policy document?
1(e)(iii)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Has the policy document been approved by the Board / Partners / Proprietor of the RE? Is the policy document reviewed by the aforementioned group periodically with a view to strengthen and improve cyber resilience posture?
1(e)(iv)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Whether the policy document is reviewed by the aforementioned group at least annually with the view to strengthen and improve its Cyber Security and Cyber Resilience framework?
1(e)(v)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Whether the Policy Approval Date is captured in the respective policy
1 (e)(vi)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Has policy version maintained for all the policy/procedure documents

Classification - Internal

1 (e)(vii)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Whether the policy approval is captured in policy/procedure documents
1 (e)(viii)	GV.PO.S1, GV.PO.S2, GV.PO.S5	1.Does the RE have policies (including but not limited to) with respect to asset management, patch management, vulnerability management, VAPT policy, audit policy, monitoring of the networks and endpoints, configuration management, change management, secure software development life cycle management, authentication policies, authorization policies and processes, network segmentation/isolation policies, commissioning internet-facing assets, encryption policies, PII and privacy policies, cybersecurity control management policy, asset ownership documentation, etc., and a chain of command for any approval process in the organization with respect to cybersecurity? 2.Do the policies contain do's and don'ts in the organization with respect to the usage of information assets including desktops, laptops, BYOD, networks, internet, data, etc. as a part of the RE's cybersecurity policy or as standalone policies? The aforementioned policies may form a part of RE's cybersecurity policy or may be standalone policies.
1 (e)(ix)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Does the Cybersecurity Policy include the following process to identify, assess, and manage cybersecurity risks associated with processes, information, networks, and systems: 1. Identify critical IT assets and risks associated with such assets. 2. Protect assets by deploying suitable controls, tools, and measures. 3. Detect incidents, anomalies, and attacks through appropriate monitoring tools/processes. 4. Respond by taking immediate steps after identification of the incident, anomaly, or attack. 5. Recover from the incident through incident management and other appropriate recovery mechanisms?
1 (e)(x)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Does the organization follow the Plan-Do-Check-Act concept while creating and using documented information, where activities under the 'Plan' phase are guided by Policies, the 'Do' phase follows Procedures (SOPs), and the 'Check' and 'Act' phases refer to the Policies and Procedures?
1 (e)(xi)	GV.PO.S1, GV.PO.S2, GV.PO.S5	As part of compliance management with respect to CSCRF, Whether the RE has applied the following key aspects (including but not limited to) for implementing compliance management:

Classification - Internal

		1. Assess Compliance with applicable guidelines/policies/laws/circulars/regulations, etc., issued by SEBI or GoI. 2. Develop compliance policies and procedures 3. Implement controls such as security measures 4. Train employees 5. Monitor and review compliance management processes 6. Regular audits and reporting while the Auditor must list all applicable implementations of Circulars, Notices, Guidelines, and advisories published by CERT-In, CSIRT-Fin Advisories, SEBI, and Exchanges/Depositories.
1 (e)(xii)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Whether the Board/Partners/Proprietor of the RE has constituted an IT Committee for REs comprising experts proficient in technology? Does this IT Committee of REs meet on a periodic basis to review the implementation of the cybersecurity and cyber resilience policy approved by their Board/Partners/Proprietor, and does such review include goal setting for a target level of cyber resilience, and establishing a plan to improve and strengthen cybersecurity and cyber resilience? Is the review placed before the Board/Partners/Proprietor of the RE for appropriate action?
1 (e)(xiii)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Does the aforementioned committee and the senior management of the RE, including the CISO, periodically review instances of cybersecurity incidents/attacks, if any, domestically and globally, and take steps to strengthen cybersecurity and cyber resilience? Does the RE seek guidance from IT committee for mitigating risks emanating from AI-led vulnerability detection models? Has the RE prepared a long-term plan for usage of AI in detection and autonomous/agentic mitigation? Whether has RE undertaken other measures including recalibration of risks for AI accelerated threats, AI augmented SOC transformation, and continuous vulnerability management using AI tools?
1 (e)(xiv)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Whether the RE has incorporated best practices from standards such as ISO 27001, ISO 27002, etc., or their subsequent revisions, if any, from time to time?
1(f)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Whether policy document have considered the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organization (NTRO), Government of India (titled 'Guidelines for Protection of National Critical Information Infrastructure') and subsequent revisions, if any, from time to time.

Classification - Internal

1(g)	GV.OC.S2, GV.OC.S3	Does the RE define and document roles and responsibilities of its employees, outsourced staff, and employees of vendors, members or participants and other entities, who may have privileged access or use systems/networks of the stockbroker/depository participants towards ensuring the goal of cybersecurity?
1(h)	GV.OV.S4	Whether the RE has conducted self-assessments of its cyber resilience using CCI and submit corresponding evidence to its submission authority annually? Is CCI and its calculation methodology done as outlined in (Annexure-K) of SEBI CSCRF? Whether the RE has strived to build an automated tool and suitable dashboards (preferably integrated with a log aggregator) for submitting compliance of CCI? Is a dashboard available at the time of cyber audit, onsite inspection/audit by SEBI or any agency appointed by SEBI?
1(i)	PR.IP.S1	Has the RE ensured that IT, OT, and IS infrastructure is 'secure by design', 'secure by engineering/ implementation', and that the infrastructure has appropriate elements to ensure 'secure IT operations'?
1(j)	PR.IP.S4, PR.IP.S6	Before introducing new technologies for critical systems, has the RE ensured that the IT/security team has assessed evolving security concerns and achieved a fair level of maturity with such technologies before incorporating them into IT infrastructure?
1(k)	PR.MA.S3	Is the procurement of hardware/software aligned with the technology refresh policy of the RE?
1(l)	RS.MA.S1	Has the RE formulated an up-to-date CCMP in line with the national CCMP of CERT-In?
1(l)(i)	RS.MA.S1	Has the CCMP been approved by the Board/Partners/Proprietor of the RE?
1(m)	RS.IM.S2	Have the updates and changes in the contingency plan, COOP, training exercises, and incident response and recovery plan been communicated and approved by the Board/Partners/Proprietor?
1(n)	RC.CO.S1, RC.CO.S2, RC.CO.S3	Has the RE discussed recovery plans with the IT Committee for REs? Do the plans include stakeholders' coordination in the recovery process, and both internal and external communication?
1(o)	PR.IP.S3	Is the change management process part of all agreements with third-party service providers to ensure that changes to the system are implemented in a controlled and coordinated manner? Whether any change in the systems (including minor changes) encompass full documentation, thorough impact analysis,

Classification - Internal

		structured review, rigorous testing and secure deployment to ensure operational resilience and system stability?
1(o)(i)	PR.IP.S3	Does the Change Management process include (but not limited to) submission, planning (impact analysis, rollout plan), approval, implementation, review (post-implementation), closure, etc.?
1(o)(ii)	PR.IP.S3	Does the RE have a clearly defined framework for change management including requirements justifying exception(s), duration of exception(s), the process of granting exception(s), and authority for approving and for periodic review of exception(s) given?
1 (p)	PR.IP.S14	Periodic Audit 1.Has the RE engaged only CERT-In empanelled IS auditing organizations for conducting external audits, including cyber audits, to audit the implementation of all standards mentioned in this framework? 2.Has the CERT-In empanelled IS auditing organization been changed after three consecutive years? 3.Along with the cyber audit reports, has the RE also submitted a declaration from the Managing Director (MD)/Chief Executive Officer (CEO) as mentioned in SEBI CSCRF? 4.Does the audit management process of the RE include (but not limited to) audit program/calendar, planning, preparation, delivery, evaluation, reporting, and follow-up, etc.? 5.For conducting audits, are CERT-In 'IT Security Auditing Guidelines for Auditee Organizations' followed by the RE? Additionally, are CERT-In 'Guidelines for CERT-In Empanelled IS Auditing Organizations' (as outlined SEBI CSCRF) mandated for empanelled IS auditing organizations? 6.Is due diligence with respect to the audit process and the tools used for such audits undertaken by RE to ensure the competence and effectiveness of audits?
1(q)	EV.ST.S1, EV.ST.S2, EV.ST.S3	Does the RE proactively assess and take necessary actions with respect to its system's requirements, architecture, design, configuration, acquisition processes, or operational processes as a strategy for adaptation to the identified and prospective threats and vulnerabilities?
1(q)(i)	EV.ST.S1, EV.ST.S2, EV.ST.S3	Does the RE strive to rapidly deploy and integrate existing and new services, both on-premises and in the cloud?
1(r)	PR.IP.S17	Does the RE follow the latest version of CIS Controls or equivalent standards, which are

Classification - Internal

		prioritized sets of safeguards and actions for cyber defense and provide specific and actionable ways to mitigate prevalent cybersecurity incidents/attacks?
1(s)	PR.MA.S3	Has the RE established a patch management policy to ensure that all applicable patches (at both PDC and DR Site) are identified, assessed, tested, and applied to all IT systems/applications in a timely manner? Has the policy been approved by the IT Committee for REs? Additionally, is the above-mentioned policy on patch management reviewed by the IT Committee for REs on an annual basis?
1(t)	DE.DP.S4	Have the results of the red teaming exercise been placed before the IT Committee for REs and the Governing board? Have the lessons learned from conducting such red team exercises been shared with SEBI within 3 months of completing the exercise? Is the status of the remediation of the observations found during the red team exercise monitored by the IT Committee for REs?
1(u)	RS.CO.S2	Does the IT Committee for REs discuss response plans, coordination with stakeholders for consistency in response actions, information sharing for better awareness, etc.?
1(v)	RC.RP.S2	Have the results of the Cyber resilience testing been placed before the IT Committee for REs? Have the lessons learned from conducting such cyber resilience testing been shared with SEBI within 3 months from the end of the relevant period of conducting cyber resilience testing? Is the status of the observations found during the cyber resilience testing being monitored and tracked by the IT Committee for REs?
2	**Identification**	
2(a)	GV.SC.S5	Has the RE obtained SBOM for their existing critical systems within 6 months (starting from the date of applicability of SEBI CSCRF)?
2(a)(i)	GV.SC.S5	Has the RE obtained SBOMs for any new critical systems software products/Software-as-a-Service applications (SaaS) at the time of procurement? Do SBOMs containing information such as all the open source and third-party components present in a codebase, versions of the components used in the codebase, and their patch status, etc., allow security teams to quickly identify any associated security or license risk?
2(a)(ii)	GV.SC.S5	Whether the SBOM obtained has included (but not limited to) the following?: 1. License information 2. Name of the supplier 3. All primary (top level) components with all

Classification - Internal

		their transitive dependencies(including third-party dependencies whether in-house or open-source components) and relationships 4. Encryption used 5. Access control 6. Cryptographic hash of the components 7. Frequency of updates 8. Known unknown (where a SBOM does not include a full dependency graph) 9. Methods for accommodating occasional incidental errors 10. All software/ applications required for core and critical business operations (irrespective of in-house or third-party) shall have a SBOM which documents all (but not limited to) components, dependencies, data relationships, etc.
2(a)(iii)	GV.SC.S5	Are Software Bill of Materials (SBOM) regularly reviewed for open-source and third-party components, with documented risk assessments and update processes in place?
2(b)	ID.AM.S1, ID.AM.S4	Has the RE identified and classified critical systems as defined in the SEBI CSCRF framework based on their sensitivity and criticality for business operations, services, and data management? Is the list of critical systems approved by the Board/Partners/Proprietor of the RE?
2(b)(i)	ID.AM.S1, ID.AM.S4	Has the RE maintained an up-to-date inventory of their (including but not limited to) hardware and systems, software, digital assets (such as URLs, domain names, applications, APIs, etc.), shared resources (including cloud assets), interfacing systems (internal and external), details of its network resources, connections to its network, and data flows?
2(b)(ii)	ID.AM.S1, ID.AM.S4	Has any additions/deletions or changes in existing assets reflected in the asset inventory within 3 working days?
2(b)(iii)	ID.AM.S1, ID.AM.S4	For conducting criticality assessment of assets, Whether the RE has taken the following steps (including but not limited to): 1. Maintain a comprehensive asset inventory 2. Conduct threat modelling (based on risk assessment) 3. Conduct vulnerability assessment
2 (c)	ID.RA.S1, ID.RA.S2	Risk Management: Does the RE conduct a risk assessment in consultation with their IT committee (including post-quantum risks) of the IT environment of their organization on a yearly basis to acquire visibility and a reasonably accurate assessment of the overall cybersecurity risk posture? Is the aforementioned risk

Classification - Internal

		assessment utilized by the RE to develop a quantifiable cybersecurity risk score?
2 (c)(i)	ID.RA.S1, ID.RA.S2	Has the RE accordingly identified cyber risks that they may face, along with the likelihood of associated threats and their impact on their business, and deployed controls commensurate to their criticality?
2 (c)(ii)	ID.RA.S1, ID.RA.S2	Does Risk Assessment include (but not limited to): 1. Technology stack and solutions used 2. Known vulnerabilities 3. Dependence on third-party service providers 4. Data storage, security and privacy protection 5. Threats, likelihoods and associated risks
2(d)	ID.AM.S6	Are all IT assets inventoried in the ITSM tool? Has the RE integrated cybersecurity considerations into product life cycles?
2 (e)	PR.AA.S6	Is an effective authentication policy implemented with the defined complexity of the password? Are all generic user IDs and email IDs which are not in use removed after the use?
3	**Protection**	
3(a)	GV.SC.S5	Whether encryption is used? Whether access control is in place?
3(b)	PR.AA.S6	Has the RE implemented strong password controls for users' access to systems, applications, networks, and databases, etc.? Do password controls include (but not limited to) a change of password upon first login, minimum password length and history, password complexity as well as maximum validity period? Is the user credential data stored using strong hashing algorithms?
3 (c)	PR.AT.S3	Does RE provide access to mobile and web applications to a customer only at her/ his option based on specific written or authenticated electronic requisition along with a positive acknowledgement of the terms and conditions?
4	**Risk Management**	
4(a)	GV.RM.S1, GV.RM.S2	A) Whether the design of the cyber risk management framework has considered the following (including but not limited to): 1. Identification of the cybersecurity risk for the organization 2. Classification of identified and mapped business functions, supporting processes, and information assets at risk. 3. Determination of risk appetite for IT and cybersecurity risks. 4. Definition of mitigation measures and

Classification - Internal

		controls to reduce the risks. 5. Monitoring of the effectiveness of the above-mentioned measures and controls. 6. Evaluation of the effect of major changes and significant operational, technical, or cybersecurity incident(s) on the risks? B) Whether the RE has used the latest version of ISO 27005 as a guidance on design, implementation, and maintenance of information security risk management? C) Does the risk management strategy of the RE include (but not limited to) risk assessment, risk analysis, risk mitigation, risk monitoring and review, compliance with relevant laws and regulations, communication of risk management policies to all stakeholders, effective mitigation measures with options for compensatory controls wherever feasible, measures to reduce residual risk and ensuring that the cybersecurity risk tolerance is within acceptable limits?
(a)(i)	GV.RM.S1, GV.RM.S2	1.Does the RE utilize metrics such as Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), Mean Time to Contain (MTTC), the number of cybersecurity incidents/intrusion attempts detected and resolved within a specific period, the number of false positives and false negatives generated by cybersecurity monitoring tools, the number of successful cyber attacks in the past year, and the measures taken to reduce these numbers through continuous refinement of the monitoring process to assess their cybersecurity maturity level? 2.Does the RE periodically assess the level of employee cybersecurity awareness, for e.g., through phishing test success rates, etc.? 3.Does the RE undertake periodic IT asset management for functions such as the number of devices on the network running end-of-life (EOL) software, the number of devices no longer receiving security updates, unidentified devices on the internal network, the integration of third-party devices and services into the network, etc.? Further, is IT asset management also utilized for the process of managing assets' access and permissions, patching cadence, security rating, third-party security rating, the number of known vulnerabilities, etc.? 4. Is a risk-based transaction monitoring or surveillance process implemented as part of

Classification - Internal

		the fraud risk management system across all delivery channels?
4(b)	GV.RM.S3	1. Is comprehensive scenario-based testing conducted to assess the cybersecurity risks of the RE? REs shall prepare their own attack scenarios as per their business model and assess their risks accordingly. The capability of AI based models may also be considered as one of the risk scenarios.
4 (c)	ID.RA.S4	1. Is a risk assessment of authentication-based solutions conducted to gain insights into the context behind each login attempt? Additionally, does the risk-based authentication solution analyze factors such as device, location, network, and sensitivity when a user attempts to sign in?
5	**Physical Security**	
5(a)	PR.AA.S10, PR.AA.S11, PR.AA.S12	Physical Security 1. Is physical access to critical systems restricted to a minimum and provided only to authorized officials? 2. Is physical access provided to third-party service providers properly supervised by ensuring that third-party service providers are accompanied at all times by authorized employees? 3. Are employees of the RE screened before being granted access to organizational information and information systems? 4.Is physical access to critical systems revoked immediately when it is no longer required? 5.Has the RE ensured that the perimeter of the critical equipment rooms, if any, is physically secured and monitored by employing physical, human, and procedural controls such as security guards, CCTVs, card access systems, mantraps, bollards, etc., wherever appropriate?
6	**Access Control**	
6(a)	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	1.Does any person, by virtue of rank or position have any intrinsic right to access confidential data applications, system resources, or facilities? 2.Is access to RE systems, applications, networks, and databases granted for a defined purpose and period? 3.Is access to IT systems, applications, databases, and networks granted on a need-to-use basis and based on the principle of least privilege? Are such access provided for a specific duration using effective authentication mechanisms? 4.Are user access rights, delegated access, unused tokens, and privileged users' activities reviewed periodically?

Classification - Internal

		5. Is access to external cloud services such as Dropbox, Google Drive, iCloud, OneDrive, etc., given as per RE's policy? 6.Are account access lock policies implemented for all accounts after a certain number of failed login attempts? 7.Are existing user accounts and access rights periodically reviewed by the system owner to detect dormant accounts, accounts with excessive privileges, unknown accounts, or any discrepancies? 8.Are proper 'end of life' mechanisms adopted for user management to deactivate access privileges of users who are leaving the organization or whose access privileges have been withdrawn? Does this include named user IDs, default user IDs, and generic email IDs?
6(a)(i)	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	1.Is Privileged Identity Management (PIM) solution or process implemented to monitor and manage privileged access? 2. Does RE implement an access policy that includes strong password controls for users' access to systems, applications, networks, and databases? 3. REs shall formulate an Internet access policy to monitor and regulate the use of internet and internet based services such as social media sites, cloud-based internet storage sites, etc. within the critical IT infrastructure of REs. 4. Does RE deploy controls and security measure RE to supervise staff with elevated system access entitlements (such as admin or privileged users)?Do such controls and measure RE include Restricting the number of privileged users, periodic review of privileged users' activities, disallow privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.? Do RE deploy controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users)?Do such controls and measures include restricting the number of privileged users, periodic review of privileged users' activities, disallow privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.?
6(b)	PR.AA.S4,	1. Does the REs have implemented suggested strategies/ methodologies such as Zero-trust networks, segmentation, no single point of failure, high availability, etc. and the same have been approved by IT committee for REs?

Classification - Internal

		2. Are delegated access and unused tokens reviewed and cleaned at least on a quarterly basis?
6 (c)	PR.AA.S16, PR.AA.S17	Is access management, including effective authentication and authorization, implemented to ensure that only the authorized RE can access the APIs?
6 (c)(i)	PR.AA.S16, PR.AA.S17	Does the mobile application undergo re-authentication whenever the device remains unused for a designated period and each time the investor/user launches the application?
6 (d)	PR.MA.S2	Has REs ensured a proper remote access policy framework that incorporates the specific requirements for securely accessing enterprise resources (located in the data center) from home using an internet connection?
7	**Network Security Management**	
7(a)	ID.AM.S1, ID.AM.S4	Has the RE prepared and maintained an up-to-date network architecture diagram at the organizational level including wired and wireless networks?
7(b)	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7,PR.AA.S9	1. Do all critical systems accessible over the internet have multi-factor security measures (such as VPNs, firewall controls, etc.) and multi-factor authentication (MFA)? 2.Is MFA enabled for all users and systems that connect using online/internet facilities, particularly for VPNs, webmail, and accounts that access critical systems from non-trusted environments to trusted environments?
7(b)(i)	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	**Network Security Management** 1. Are adequate controls deployed to address virus, malware, and ransomware attacks on servers and other IT systems? Do these controls include host/network/application-based Intrusion Prevention Systems (IPS), customized kernels for Linux, anti-virus, and anti-malware software? Are anti-virus definition file updates and automatic anti-virus scanning performed regularly? 2. Has the RE established baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices, enterprise mobile devices, etc., within the IT environment? Does the RE also conduct regular enforcement checks to ensure that baseline standards are applied uniformly? 3. Are the LAN and wireless networks within the organization's premises secured with proper access controls? 4.Does the RE limit the total and maximum connections to the SMTP server?

Classification - Internal

7(b)(ii)	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	**Network Security Management** 1. Has the RE applied appropriate network segmentation and isolation techniques to restrict access to sensitive information, hosts, and services? Is segment-to-segment access based on a strong access control policy and the principle of least privilege? 2. Has the RE installed network security devices, such as Web Application Firewalls (WAF), proxy servers, and Intrusion Prevention Systems (IPS), to protect their IT infrastructure exposed to the internet from security threats originating from internal and external sources? 3. Has the RE deployed web and email filters on the network? Are these devices configured to scan for known bad domains, sources, and addresses, block these before receiving and downloading messages, filter out emails with known malicious indicators (such as known malicious subject lines), and block suspicious IP addresses and malicious domains/URLs at the firewall? Are all emails, attachments, and downloads scanned with a reputable antivirus solution both on the host and at the mail gateway? 4. Are network devices configured in line with the whitelist approach of IPs, ports, and services for inbound and outbound communication with proper Access Control List (ACL) implementation? 5. Has the RE implemented DNS filtering services to ensure only clean DNS traffic is allowed in the environment? Is DNS security extension used for secure communication? Is the management of critical servers, applications, services, and network elements restricted through enterprise-identified intranet systems? 6. Has the RE implemented Sender Policy Framework (SPF), Domain- based Message Authentication, Reporting & Conformance (DMARC), and DomainKeys Identified Mail (DKIM) for email security? 7. Does email protection include best practices such as strong password protection, multi-factor authentication (MFA), spam filtering, email encryption, a secure email gateway, and permissible attachment types? 8. Has the RE blocked malicious domains and IPs after diligent verification without impacting operations? Are CSIRT-Fin/CERT-In advisories, which are published periodically, referred to for the latest malicious domains, IPs, Command & Control (C&C) DNS, and links? 9. Does the RE maintain an up-to-date and centralized inventory of authorized devices

Classification - Internal

		connected to their network (both within and outside the RE premises) and authorized devices enabling the network? Does the RE implement solutions to automate network discovery and management?
7(c)	PR.AA.S10,PR.AA.S11, PR.AA.S12	**Remote Support Service Security** 1. As many OEMs and their service partners, as well as System Integrators, provide remote support services to organizations, does the RE ensure that these services are well-governed, controlled, logged, and that oversight is maintained on all the activities done by remote support service providers? Are the above complemented by regular monitoring and audit to ensure compliance with the defined policies for privileged users and remote access? 2. Does the RE ensure secure usage of RDP in IT systems? Is it implemented strictly on a need-to-use basis and does it employ MFA? Is remote access, if necessary, given to authorized personnel from whitelisted IPs for a predefined time period, with a provision to log all activities? 3. Are employees and third-party service providers who may be given authorized access to the critical systems, networks, and other IT resources of REs subject to stringent supervision, monitoring, and access restrictions?
7(d)	PR.AA.S15	**Endpoint security** 1. Are solutions like Endpoint Protection Platforms (EPP), Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), and anti-malware software implemented to detect threats and attacks on endpoint devices, and to enable immediate response to such threats and attacks? Does the RE ensure that signatures are updated on all IT systems? 2. Are solutions like Intrusion Prevention Systems (IPS) and Next- Generation Intrusion Prevention Systems (NG-IPS) used to continuously monitor the organization's network for malicious activities?
7 (e)	PR.AA.S16, PR.AA.S17	Has RE ensured connection to entities via APIs being strictly based on a whitelist approach?
7 (e)(i)	PR.AA.S16, PR.AA.S17	1.Does the mobile application check new network connections or connections for unsecured networks like VPN connections, proxy, and unsecured Wi-Fi connections?
7(f)	PR.IP.S1	1. Is the practice of whitelisting ports based on business usage implemented at the firewall level, rather than blacklisting certain ports? Is traffic on all other ports that have not been whitelisted blocked by default?

Classification - Internal

		2. Does the RE utilize host-based firewalls to prevent Remote Procedure Call (RPC) and Server Message Block (SMB) communications among endpoints wherever possible to limit lateral movement and other attack activities?
7(g)	5(k)	1. Is the Network Time Protocol (NTP) server configured to be synchronised with National Physical Laboratory (NPL) or National Informatics Centre (NIC) or any associated servers for synchronisation of all ICT system clocks?
7(h)	PR.MA.S2	1. Does the RE ensure that only trusted client machines are permitted to access enterprise IT resources remotely? Has the RE put in place appropriate security control measures such as (including but not limited to) host integrity check, binding of the MAC address of the device with the IP address, etc., for remote access and telecommuting? Has the RE ensured that appropriate risk mitigation mechanisms are put in place whenever remote access of data center resources is permitted for third-party service providers?
7(i)	PR.AA.S1, PR.AA.S2, PR.AA.S3	Depository Participants shall take adequate measures to isolate and secure the perimeter and connectivity to the servers running for DP related applications
8	**Data security**	
8(a)	PR.DS.S4	Does the RE enforce effective data protection, backup, and recovery measures?
8(a)(i)	PR.DS.S4	Has the RE implemented measures to control the usage of VBA/macros in office documents and control permissible attachment types in email systems?
8(a)(ii)	PR.DS.S4	Does the RE have a documented data migration policy specifying SOPs and processes for data migration while ensuring data integrity, completeness, and consistency?
8(b)	PR.AA.S15	**Restricted Use of Removable Media and Electronic Devices** 1.Has the RE defined and implemented a policy for restriction and secure use of removable media (such as USB, external hard disks, etc.) and electronic devices (such as laptops, mobile devices, etc.)? 2. Does the RE ensure secure erase of data so that no data is in recoverable form on such media and electronic devices after use?
8 (c)	PR.AA.S16, PR.AA.S17	1.Does the mobile application store/retain sensitive personal/investor authentication information such as user IDs, passwords, keys, hashes, hardcoded references, etc., on the device? Does the application securely wipe out any sensitive investor/user information from

Classification - Internal

		memory when the investor/user exits the application?
8(d)	PR.DS.S1, PR.DS.S2,PR.DS.S3	**Data and Storage Devices Security** 1.Is data encrypted in motion, at rest, and in-use by using strong encryption methods? 2. Whether data-in-use encryption for cloud deployments as per reference mentioned in Annexure J of **SEBI circular No. SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024** is followed or not? 3. Is layering of Full-disk Encryption (FDE) along with File-based Encryption (FBE) used wherever possible? 4. Does the RE use industry-standard, strong encryption algorithms (e.g., RSA, AES, etc.) wherever encryption is implemented? 5. Are the illustrative measures given in Annexure-H and Annexure-I of CSCRF circular been provided for data security on customer-facing applications and data transport security being implemented? 6. Have Data Loss Prevention (DLP) solutions or processes been deployed by the RE? 7.Has the RE implemented measures to prevent unauthorized access, copying, and transmission of data/information held in contractual or fiduciary capacity? 8. Does the RE ensure that the confidentiality of information is not compromised during the process of exchanging and transferring information with external parties? 9.Are the illustrative measures been provided in data transport security to ensure the security of data during internet transmission being implemented? 10. Does the information security policy cover the use of devices such as mobile phones, photocopiers, scanners, etc., which can be used for capturing and transmission of sensitive data within their IT infrastructure? 11.Are access policies for personnel and network connectivity for such devices defined? 12. Does the RE allow only authorized data storage devices within their IT infrastructure through appropriate validation processes?
9	**Hardening of Hardware and Software**	
9(a)	PR.DS.S4	Does the RE block administrative rights on end-user workstations/PCs/laptops by default and provide access rights on a need basis as per the established process and approvals and for the specific duration for which it is required?
9(b)	PR.IP.S1	Does the implementation of the principle of least functionality include measures such as configuring only essential capabilities by disabling unnecessary and/or unsecured

Classification - Internal

		functions, ports, protocols, services, etc., within the information system?
9(b)(i)	PR.IP.S1	**Hardening of Hardware and Software** 1.Does the RE deploy only hardened and vetted hardware/software? During the hardening process, does the RE, inter-alia, ensure that default usernames and passwords are replaced with non-standard usernames and strong passwords, and all unnecessary services are removed or disabled in software/systems? 2. Has OS hardening been done to protect servers'/endpoints' OS and minimize attack surface and exposure to threats? 3.Does the RE ensure that for running services, non-default ports are used wherever applicable? Has the RE blocked open ports on networks and systems that are not in use or could potentially be exploited? Does the RE monitor all open ports and take appropriate measures to secure them? 4.Has the RE restricted the execution of "PowerShell" and "wscript" in their environment, if not required? Additionally, has the RE installed the latest version of PowerShell, with enhanced logging enabled, script block logging, and transcription enabled? Are the associated logs being sent to a centralized log repository for monitoring and analysis?
9(b)(ii)	PR.IP.S1	Does the RE use application directory whitelisting on all assets to ensure that only authorized software is run and all unauthorized software is blocked from installation/execution?
9 (c)	PR.AA.S15	Are the PowerShell and local admin rights disabled by default on endpoint machines and used only for a specific purpose and for a limited time?
9(d)	EV.ST.S1,EV.ST.S2,EV.ST.S3	Does the RE strive to reduce their attack surfaces?
9(d)(i)	EV.ST.S1,EV.ST.S2,EV.ST.S3	Does the RE look for the feasibility of deploying diverse operating systems? Would an attack or compromise on one type of OS affect other OSs deployed?
10	**Application Security in Customer Facing Applications**	
10(a)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Has the RE formulated a policy for mobile and web applications and associated services with the approval of their Board/Partners/Proprietor? Do the contours of the policy, while discussing the parameters of any "new product" including its alignment with the overall business strategy and inherent risk of the product, risk management/mitigation measures, compliance with regulatory instructions, customer experience, etc.,

Classification - Internal

		explicitly include security requirements from Functionality, Security, and Performance (FSP) angles?
10(b)	PR.AT.S3	Has the RE mentioned/incorporated a section on the mobile and web application clearly specifying the process and procedure (with forms/contact information, etc.) to lodge customer/investor grievances with respect to technology-related issues and cybersecurity? Has a mechanism been put in place to keep this information periodically updated? Does the reporting facility on the application provide an option for registering a grievance? Is customers'/investors' dispute handling, reporting, and resolution procedure, including the expected timelines for response, clearly defined?
10(b)(i)	PR.AT.S3	Does RE mention/incorporate a section on the mobile and web application clearly specifying the process and procedure (with forms/contact information, etc.) to lodge customer/investor grievances with respect to technology-related issues and cybersecurity? Is a mechanism in place to keep this information periodically updated? Does the reporting facility on the application provide an option for registering a grievance?
10(b)(ii)	PR.AT.S3	Does the RE provide a mechanism on their mobile and web application for their customers/investors with necessary authentication to identify/mark a transaction as fraudulent for seamless and immediate notification to his entities? On such notification by the customer/investor, do they endeavor to build the capability for seamless/instant reporting of fraudulent transactions to the corresponding beneficiary/counterparty's entities; vice-versa have a mechanism to receive such fraudulent transactions reported from other entities?
10 (c)	PR.DS.S4	Do the security controls for mobile and web applications focus on how these applications handle, store, and protect PII and other business-related data?
10 (c)(i)	PR.DS.S4	Do web and mobile applications store sensitive information in HTML hidden fields, cookies, or any other client-side storage to avoid any compromise in the integrity of the data?
10(d)	PR.IP.S4,PR.IP.S6	**Secure Software Development Cycle (SSDLC)** 1. Has the RE prepared business requirement documents with clear mentioning of security requirements, session management, audit trail, logging, data integrity, security event tracking, exception handling, etc.?

Classification - Internal

		2. Has the RE conducted threat modelling and application security testing during the development phase for the secure rollout of software and applications? 3.Has the RE referred to standards, security guidelines for application security and other protection measures given by OWASP (for e.g., OWASP-ASVS)? 4.Has the RE adopted the principle of defence-in-depth to provide a layered security mechanism?
10(d)(i)	PR.IP.S4,PR.IP.S6	**Secure Software Development Life Cycle (SSDLC)** 1.Does the RE undertake regression testing before new or modified systems are implemented? 2. Does the scope of these tests cover business logic, security controls, system performance under various stress-load scenarios, and recovery conditions?
10 (e)	PR.IP.S15	1. Are the tests/audits mentioned in point 1 (a-b) limited to cybersecurity aspects? Does application security testing also include API security and API discovery? 2. Does the scope of the functional audit cover data integrity, report integrity, and transaction integrity, etc.?
10(f)	PR.AA.S16, PR.AA.S17	**API Security:** 1.Does the RE use effective API security strategies like rate limiting and throttling while developing APIs to prevent overuse or abuse? 2.Does the RE have API security solutions in place for securing services and data transmitted through APIs? 3.Does the RE follow OWASP documentation for developing APIs, and are OWASP top 10 API security risks mitigated? 4.Any entity connecting to REs via APIs, is that allowed to connect strictly on a whitelist-based approach? 5. Stockbrokers / Depository Participants should maintain inventory of API with details including ownership, criticality/impact, type (external/ internal) of API, etc. 6. Stockbrokers / Depository Participants should ensure Strong Authentication Mechanisms such as API keys, OAuth, or IWT, ensuring secure token management practices and setting appropriate expiration times should be defined. 7. Centralized API Security: Establish an API gateway for centralized security enforcement and a web application firewall (WAF) to protect against common web threats. Implement an API security gateway for both internal and external APIs. Disable any public API lacking

Classification - Internal

		secure authentication or strengthen it as per advisory at the earliest. 8. Data Protection and Secure Communication: Prioritize data protection by encrypting sensitive data, applying data masking techniques and using secure communication protocols to prevent eavesdropping and information leakage. Additionally, integrity checks through checksum or digital signature should be implemented to ensure data integrity & to avoid data manipulation/MITM 9. Input Validation and Output Encoding: Validate and sanitize user inputs to prevent injection attacks and encode output to protect against HTML /JavaScript injection. 10. Rate Limiting and Throttling: Implement rate limiting and throttling mechanisms to prevent abuse and DDoS attacks, limiting requests from a single client within a specific time frame. 11. Error Handling and Logging: Ensure proper error handling and comprehensive logging for monitoring and auditing purposes. 12. Cross-Origin Resource Sharing (CORS): Configure CORS properly to restrict unauthorized cross-origin requests. 13. Secure Storage of Secrets: Do not Store or Transmit API keys, credentials and sensitive data without secure encryption and access controls. 14. Regular Security Assessments: Conduct regular security assessments, including penetration testing, security audits, and code reviews. All API's need to be assessed for security weakness /vulnerabilities and the checks should be aligned to OWASP Top 10 API security framework. 15. Documentation: Maintain clear documentation on secure API usage, including examples of proper authentication and authorization methods. For API's facilitating sensitive business flows access shall be restricted on need-to-know basis. 16. Privacy Protection: Minimize data collection to essential information, comply with relevant privacy regulations and obtain user consent for data processing. Integrate privacy considerations from the initial stages of API development, performing a Privacy Impact Assessment (PIA) to identify and mitigate potential privacy risks. 17. Secure Software Development Lifecycle (SDLC): Integrate security considerations into the entire API development process and conduct security training for developers to promote secure coding practices.

Classification - Internal

10(f)(i)	PR.AA.S16, PR.AA.S17	1. Does the mobile application implement a device-binding solution to create a unique digital identity based on the device, mobile number, and SIM? 2. Is OWASP – MASVS referred for implementing mobile application security and other protection measures? 3. Has the RE implemented measures such as installing a “containerized” app on mobile/smartphones for exclusive business use that is encrypted and separated from other smartphone data/applications? Have measures been implemented to initiate a remote wipe on the containerized app, rendering the data unreadable, in case of requirement?
10(f)(ii)	PR.AA.S16, PR.AA.S17	Guidelines for Application Security and Emerging Technologies Has the RE prepared SOPs for open source application security and concerns from emerging technologies like Generative AI security?
10(g)	PR.DS.S1, PR.DS.S2, PR.DS.S3	**Application Security in Customer Facing Applications:** 1.Does the RE address application security for customer-facing applications offered over the Internet, such as IBTs (Internet-Based Trading applications), portals containing sensitive or private information, and back-office applications (repositories of financial and personal information offered by RE to customers), given their significant attack surfaces due to public availability? 2.Is the illustrative list of measures provided in Annexure G of **SEBI circular No. SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024** for ensuring security in customer-facing applications under application authentication security being implemented?
10(h)	PR.DS.S5	Does the RE ensure that separate production and non-production environments are maintained for the development of all software/applications and feature enhancements?
10(h)(i)	PR.DS.S5	Does the RE conduct System Integration Testing (SIT) after development and/or feature enhancement to ensure that the complete software/application is working as required?
10(h)(ii)	PR.DS.S5	1. During the development phase of any software or application intended for use by RE or its customers, is it ensured that vulnerabilities identified by best practice baselines, such as OWASP Top 10 and SANS Top 25 software security vulnerabilities, are addressed? 2. Has the RE adopted methodologies such as

Classification - Internal

		DevSecOps to ensure the secure development of their applications and software?
11	**Patch management**	
11(a)	GV.SC.S5	1.Does the RE have a defined schedule for patch updates? How frequently are these updates applied to ensure the security and integrity of the software and systems?
11(b)	PR.DS.S4	Does the RE ensure that their digital certificates used in IT systems are renewed well in advance to prevent any lapses in security?
11 (c)	PR.MA.S3	Has the RE established and ensured that the patch management procedures include the identification, categorization, and prioritization of patches and updates? Is an implementation timeframe for each category of patches established to apply them in a timely manner?
11 (c)(i)	PR.MA.S3	1.Does the organization update all operating systems and applications with the latest patches on a regular basis? 2.Does the organization consider virtual patching as an interim measure for zero-day vulnerabilities when patches are not available? 3.Does the organization source patches only from the authorized sites of the OEM to ensure their authenticity and security?
11 (c)(ii)	PR.MA.S3	1.Does the RE perform comprehensive and rigorous testing of security patches and updates, wherever possible, before deployment into the production environment to ensure that the application of patches does not impact other systems?
11 (c)(iii)	PR.MA.S3	Does the organization ensure that all patches are tested first in a non-production environment that closely resembles the production environment?
11 (c)(iv)	PR.MA.S3	Does the organization ensure that hardware and software of critical systems are replaced before they reach End-of-Life or End-of-Support to maintain security and operational integrity?
11 (c)(v)	PR.MA.S3	Does the organization implement compensatory controls, such as virtual patching, for legacy systems for a maximum period of 6 months? Does the organization ensure that the constraints necessitating virtual patching are legitimate and properly documented?
11 (c)(vi)	PR.MA.S3	Does the RE ensure that post-application of any patch/update, the resources deployed are adequate enough to deliver the expected performance?
11 (c)(vii)	PR.MA.S3	Does the RE have established processes for tracking patch compliance across all IT

Classification - Internal

		systems and applications, and are these compliance reports submitted to the respective IT Committee on a quarterly basis?
11 (c)(viii)	PR.MA.S3	1. Does the RE ensure that patches are implemented at both PDC and DR sites within the following upper/maximum time limits based on their criticality: High: 1 week Moderate: 2 weeks Low: 1 month 2. For emergency patching, does the RE deploy patches within the timelines stipulated by the OEMs?
12	**Disposal of data, systems, and storage devices**	
12(a)	PR.AA.S13, PR.AA.S14	Has the RE formulated a data-disposal and data-retention policy to identify the value and lifetime of various parcels of data?
12(a)(i)	PR.AA.S13, PR.AA.S14	Has the RE framed suitable policies for disposal of storage media and systems? Is the critical data/information on such devices and systems removed by using methods such as wiping/cleaning/overwrite, degauss/crypto shredding/physical destruction as applicable?
13	**Vulnerability Assessment and Penetration Testing (VAPT)**	
13(a)	ID.AM.S1, ID.AM.S4	1.Does the organization conduct threat modelling based on risk assessment to identify and mitigate potential vulnerabilities early in the software development lifecycle? 2.Does the organization conduct regular vulnerability assessments to identify, quantify, and prioritize security weaknesses in their systems and applications?
13(b)	PR.IP.S15	1. Does the RE ensure that all categories of software solutions, applications, and products for critical systems mandatorily pass through the following tests, audits, and compliances? 2. Does the RE conduct Dynamic Application Security Testing (DAST) to scan software applications in real-time against leading vulnerability sources, such as OWASP Top 10 and SANS Top 25 CWE, to identify security flaws or open vulnerabilities? 3. Does the RE conduct Static Application Security Testing (SAST) to analyze program source code and identify security vulnerabilities such as SQL injection, buffer overflows, XML external entity (XXE) attacks, and OWASP Top 10 security risks? 4. Does the RE conduct functional audits to verify that the software meets all specified requirements and functions correctly? 5. Does the RE conduct Vulnerability Assessment and Penetration Testing (VAPT) after every major release of the application or software to identify and address security

Classification - Internal

		weaknesses? 6. Does the RE integrate logs from all critical systems with the RE Security Operations Center (SOC) to ensure comprehensive monitoring and incident response? 7. Does the RE conduct audits of firewall configuration, Web Application Firewall (WAF) configuration, token configuration, and channel identification to ensure robust security settings? 8. Does the RE generate a Software Bill of Materials (SBOM) to provide a detailed inventory of all components used in the software, enhancing transparency and security? 9. Does the RE maintain a Requirement Traceability Matrix (RTM) to ensure that all requirements are tracked throughout the development lifecycle and are met?
13 (c)(i)	DE.CM.S5	Does the RE regularly conduct cybersecurity audits and VAPT with the scope mentioned in CSCRF to detect vulnerabilities in the IT environment? Does the RE conduct in-depth evaluations of the security posture of the system through simulations of actual attacks? An indicative (but not exhaustive and limited to) VAPT scope has been attached at Annexure-L of SEBI circular No. **SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024 circular.**
13 (c)(ii)	DE.CM.S5	Do the assets under these audits include (but not limited to) all critical systems, infrastructure components (like networking systems, security devices, load balancers, servers, databases, applications, remote access points, systems accessible through WAN, LAN as well as with Public IPs, websites, etc.), and other IT systems pertaining to the operations of RE?
13 (c)(iii)	DE.CM.S5	Does the RE perform VAPT prior to the commissioning of new systems, especially those which are part of critical systems or connected to critical systems?
13 (c)(iv)	DE.CM.S5	Does the organization ensure that revalidation of VAPT is conducted in a time-bound manner post-closure of observations to confirm that all open vulnerabilities have been fixed??
13(d)	RS.AN.S4, RS.AN.S5	Does the RE conduct compromise assessments through CERT-In empanelled Information Security (IS) auditing organizations?
13 (e)	PR.AA.S15	Guidance on Usage of Active Directory (AD) Servers 1.Does the RE regularly review the Active

Classification - Internal

		Directory (AD) to locate and close existing backdoors, such as compromised service accounts, which often have administrative privileges and are potential targets of attacks? 2.Does the RE undertake penetration testing activities for known AD Domain Controller abuse attacks? 3.Does the RE remediate identified weaknesses with the highest priority?
13(f)	DE.CM.S5	Does the RE ensure they engage only CERT-In empanelled organizations for conducting VAPT? Does the RE ensure that the final report on VAPT is submitted to the Depository after approval from the Technology Committee of the respective RE within one month of completion of the VAPT activity?
13(g)	PR.IP.S4, PR.IP.S6	For any production release, is vulnerability assessment undertaken? For all major releases, does the RE conduct a VAPT to assess the risks and vulnerabilities arising from recent additions or modifications in applications/software?
13(h)	PR.IP.S14	Does the RE conduct revalidation VAPT and cyber audits in a time-bound manner to ensure that all open vulnerabilities in its IT assets have been fixed?
13(i)	EV.ST.S1,EV.ST.S2,EV.ST.S3	Does the RE anticipate new attack vectors through threat modeling (based on risk assessment) and work to defend them?
13(j)	EV.ST.S1,EV.ST.S2,EV.ST.S3	Does the RE proactively examine controls, practices, and capabilities for prospective, emerging, or potential threats?
13(j)(i)	DE.DP.S4	Does the RE conduct red teaming exercises as part of their cybersecurity framework on a half-yearly basis through the use of red/blue teams?
13(k)	DE.DP.S4	Does the RE deploy a CART solution for continuous, automated processing of testing the security of the systems and achieving greater visibility on attack surfaces?
13(k)(i)	DE.DP.S4	Does the red team for red teaming exercises consist of RE employees and/or outside experts? Additionally, is the red team independent of the function being tested?
14	**Monitoring and Detection**	
14(a)	ID.RA.S4	Measures against Phishing websites and attacks- Does the RE proactively monitor the cyberspace to identify phishing websites w.r.t. RE domains and report the same to CSIRT-Fin/CERT-In for taking appropriate action?
14(b)	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7,PR.AA.S9	Does the RE ensure that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes?

Classification - Internal

		Are such logs maintained and stored in a secure location for a time period not less than two (2) years (at least 6 months in online mode and the rest in archival mode)? Does the RE also maintain records of users with access to shared accounts?
14 (c)	PR.AA.S8	Does the RE ensure that all log sources are identified and their respective logs are collected? Additionally, does the RE collect an indicative list of log data types, including system logs, application logs, network logs, database logs, security logs, performance logs, audit trail logs, and event logs?
14 (c)(i)	PR.AA.S8	Does the RE monitor all logs of events and incidents to identify unusual patterns and behaviors?
14(d)	DE.CM.S1, DE.CM.S2,DE.CM.S3	Security Continuous Monitoring a. Has the RE established appropriate security monitoring systems and processes to facilitate continuous monitoring of security events/alerts and timely detection of unauthorized or malicious activities, unauthorized changes, unauthorized access, and unauthorized copying and transmission of data/information held in contractual or fiduciary capacity by internal and external parties? b. Does the RE monitor the security logs of systems, applications, and network devices exposed to the internet for anomalies? c. Does the RE generate suitable alerts in the event of detection of unauthorized or abnormal system activities, transmission errors, or unusual online transactions? d. To enhance security monitoring, does the RE (except client-based stock brokers having less than 100 clients) employ SOC services for their systems? e. Are small-size and self-certification REs onboarded on the above-mentioned Market SOC? f. Has RE successfully onboarded all critical systems to the SOC, ensuring all logs are integrated with the SOC?
14(d)(i)	DE.CM.S1, DE.CM.S2,DE.CM.S3	Does the RE utilizing third-party managed SOC services or market SOC obtain an SOC efficacy report from their SOC provider annually, using the quantifiable method outlined given Annexure N of **SEBI circular No. SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024** from their SOC provider on a yearly basis?
14(d)(ii)	DE.CM.S1, DE.CM.S2,DE.CM.S3	Functional efficacy of SOC: Does the RE assess the functional efficacy of their SOC using the quantifiable method as

Classification - Internal

		outlined in Annexure N of **SEBI circular No. SEBI/HO/ ITD1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024**? Does the RE review the functional efficacy of SOC on a half-yearly basis? Does REs consider deploying a range of security solutions in consultation with their IT Committee, such as threat simulation, vulnerability management, and decoy systems, to assess and enhance their cybersecurity posture?
14(d)(iii)		The auditor shall verify that, RE who have implemented/opted for Own / Group SOC (in accordance with SEBI CSCRF guidelines), are maintaining Functional efficacy of SOC & related reports as per guidelines and format provided in Annexure N of SEBI-CSCRF 2024.
14 (e)	PR.AA.S10,PR.AA.S11, PR.AA.S12	Does the RE monitor environmental controls (temperature, water, smoke, etc.), service availability alerts (power supply, servers, etc.), and access logs?
14(f)	ID.RA.S3	Does the RE engage Dark web monitoring (for brand intelligence, customer protection, etc.), and takedown services as a cyber-defence strategy to check for any brand abuse, data/credentials leak, combating cyber abuse, etc.?
14(f)(i)	ID.RA.S3	Does the RE have processes in place to manage and incorporate IOAs/ IOCs/ malware alerts/ vulnerability alerts (received from CERT-In or NCIIPC (as applicable) or any other government agencies) in their systems?
14(g)	PR.IP.S14	Does the RE strive to build an automated tool and suitable dashboards (preferably integrated with a log aggregator) for submitting compliance with CSCRF? Is a dashboard available at the time of cyber audit, onsite inspection/audit by SEBI or any agency appointed by SEBI?
14(h)	RS.AN.S1,RS.AN.S2, RS.AN.S3	Does the RE suitably investigate alerts generated from monitoring and detection systems to determine activities that should be performed to prevent the spread of cybersecurity incidents/attacks or breaches, mitigate their effects, and resolve the incidents?
14(i)	DE.CM.S4	Does RE ensure high resilience, high availability, and timely detection of attacks on systems and networks exposed to the internet by implementing suitable mechanisms to monitor capacity utilization of its critical

Classification - Internal

		systems and networks, such as using firewalls to monitor bandwidth usage?
14(j)	PR.DS.S1, PR.DS.S2, PR.DS.S3	Does RE implement suitable mechanisms, including the generation of appropriate alerts, to monitor capacity utilization on a real-time basis and proactively address issues pertaining to their capacity needs? For capacity planning and monitoring, REs shall comply with circulars/ guidelines on capacity planning issued by SEBI & exchanges/Depositories (and updated from time to time).
14(k)	PR.MA.S2	Does the RE ensure that remote access is monitored continuously for any abnormal/unauthorized access, and appropriate alerts and alarms are generated to address this breach before any damage is done?
14(l)	DE.CM.S4	a.Is the use of IT assets/resources monitored, tuned, and are projections made for future capacity requirements to ensure the required system performance for meeting the business objectives? b.To ensure high resilience, high availability, and timely detection of attacks on systems and networks, does the RE implement suitable mechanisms to monitor capacity utilization of its critical systems and networks? Does the RE's capacity management comprise of three primary types; Data storage capacity – (e.g., in database systems, file storage areas, etc.), Processing power capacity – (e.g., adequate computational power to ensure timely processing operations), Communications capacity – (“bandwidth” to ensure communications are made in a timely manner). c.Is capacity management: Proactive – for example, using capacity considerations as part of change management? Reactive – e.g., triggers and alerts for when capacity usage is reaching a critical threshold so that timely increments (temporary or permanent) can be made?
14(m)	EV.ST.S1,EV.ST.S2, EV.ST.S3	6. Does the RE strive to rapidly correlate data using mathematical models and machine learning in order to make data-driven decisions?
14(m)(i)	EV.ST.S1,EV.ST.S2,EV.ST.S3	7. Does the RE use auditing/logging systems on different OS to acquire and store audit/logging data?

Classification - Internal

14(m)(ii)	EV.ST.S1,EV.ST.S2,EV.ST.S3	8. In order to include heterogeneity, are different audit/logging regimes applied at different architectural layers?
14(n)	DE.DP.S5	Does the RE proactively search for hidden and undetected cyber threats in their network?
14(o)	DE.DP.S5	Is threat hunting by leveraging threat intelligence, IOCs, IOAs, etc., conducted on a quarterly basis?
14(p)	RS.MA.S5	Reporting of Cybersecurity Incidents Does the RE collaborate with Cyber Swachhta Kendra (CSK) operated by CERT-In to trace bots and vulnerable service(s) running on their public IP addresses, and receive alerts regarding the same? Are the alerts received from CSK closed in a time-bound manner? Are observations (from CSK) which require a longer time to close put up to the IT Committee for REs for their guidance and appropriate mitigation/closure?
14(q)	DE.CM.S5	In case of vulnerabilities discovered in COTS (used for core business) or empanelled applications, does the RE report them to the vendors and the designated stock exchanges and/ or depositories in a timely manner?
15	**Response and Recovery**	
15(a)	GV.OC.S2	Does the RE engage a forensic auditor to identify the root cause of any incident (cybersecurity or other incidents) related to the RE?
15(b)	RS.MA.S1	i.Has the RE developed an Incident Response Management Plan as part of their CCMP? ii.Does the response plan define responsibilities and actions to be performed by the RE employees and support/outsourced staff in the event of a cyberattack or cybersecurity incident? iii.Does the RE have an SOP for handling cybersecurity incident response and recovery for the various cybersecurity attacks? iv.Whether SOP as per Annexure -O of **SEBI circular No. SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024** circular is adhered or not?
15 (c)	RS.CO.S1,RS.CO.S2,RS.CO.S3	During the processing of reported incidents by SEBI, does the RE provide regular reports (such as RCA, forensic analysis report, etc.) on the progress of the incident analysis?
15(d)	RS.CO.S2	Does the RE notify the customer/investor, through alternate communication channels, of all transactions including buy/sell, payment or fund transfer above a specified value determined by the customer/investor?
15(d)(i)	RS.CO.S2	For the purpose of coordinating incident response, does the RE regularly update the

Classification - Internal

		contact details of service providers, intermediaries, and other stakeholders?
15(d)(ii)	RS.CO.S2	If the cyberattack is of high impact and has a broad reach, does the REs had taken action as per their approved Cyber Crisis Management Plan (CCMP)?
15(d)(iii)	RS.CO.S2	If the cyberattack is of low impact and has a narrow/low reach, does the RE inform all the affected customers/stakeholders?
15 (e)	RS.AN.S1,RS.AN.S2, RS.AN.S3	Data collection: Does the RE collect and preserve data related to the incident, such as system logs, network traffic, and forensic images of affected systems?
15 (e)(i)	RS.AN.S1,RS.AN.S2, RS.AN.S3	Incident Analysis: Does the RE analyze the data to understand the scope, cause, and impact of the incident, including how the incident occurred, what systems and data were affected, who was responsible, etc.?
15 (e)(ii)	RS.AN.S1,RS.AN.S2, RS.AN.S3	Evidence Preservation: Does the RE preserve evidence related to the incident, including digital artifacts, network captures, and memory dumps, in a secure and forensically sound manner?
15(f)	RS.AN.S4, RS.AN.S5	Root Cause Analysis: Does the RE perform a root cause analysis (RCA) to identify the specific control that has failed, the underlying cause of the incident, and the potential areas of improvement?
15(f)(i)	RS.AN.S4, RS.AN.S5	Forensic: Is forensic analysis (as appropriate) undertaken by the RE?
15(f)(ii)	RS.AN.S4, RS.AN.S5	Are incidents of loss or destruction of data or systems thoroughly analyzed, and are lessons learned from such incidents incorporated to strengthen the security mechanisms and improve the recovery planning and processes?
15(f)(iii)	RS.AN.S4, RS.AN.S5	Reporting: Does the RE create a detailed incident report that includes information on the scope, cause, and impact of the incident, as well as recommendations for improving incident response and recovery capabilities?
15 (g)	RS.IM.S1	Does the RE periodically review and update their contingency plan, COOP, training exercises, and incident response and recovery plans (including CCMP) to incorporate lessons learned, and strengthen their response capabilities in the event of a future incident/attack?
15 (g)(i)	RS.IM.S1	Post-occurrence of a cybersecurity incident (if any), does the RE update their response and recovery plan (including CCMP) to improve their cyber resilience and incorporate the learnings from the cybersecurity incident?

Classification - Internal

15(h)	RC.RP.S1	Do the response and recovery plans of the RE include scenario-based classifications? Does the RE build their own response and recovery plan as per their business model and include the same in their CCMP?
15(h)(i)	RC.RP.S1	Does the response and recovery plan of the RE include plans for the timely restoration of systems affected by cybersecurity incidents/attacks or breaches (for instance, offering alternate services or systems to customers)? Are tests designed to challenge the assumptions of response, resumption, and recovery practices, including governance arrangements and communication plans? Do these tests include all stakeholders such as critical service providers, vendors, other linked REs, etc.?
15(h)(ii)	RC.RP.S1	Is an indicative (but not exhaustive) recovery plan for the RE included in Annexure C of of **SEBI circular No. SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024** followed or not?
15(h)(iii)	RC.RP.S1	Has the RE maintain regularly updated "golden images" of critical systems at off-site locations for rebuilding the systems (whenever required)? Does this entail maintaining images “templates” that include a preconfigured operating system (OS), configuration setting backup, and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server?
15(h)(iv)	RC.RP.S1	Has the RE explore the possibility of retaining spare hardware in an isolated environment to rebuild systems in an event that starting RE operations from PDC and/or DRS is not feasible? Does the RE also try to keep spare hardware in a ready-to-use state for delivering critical services, and are such systems updated as and when new changes (for example, OS patches, security patches, etc.) are implemented in the primary systems? Does this spare hardware regularly undergo testing in line with the response and recovery plan of the RE?
15(h)(v)	RC.RP.S1	Does Qualified RE has maintained spare hardware in ready-to-use state for delivering critical services, as it is mandated and as their business is critical to Indian securities market ecosystem?
15(h)(vi)	RC.RP.S1	Has the RE take all necessary precautions while updating the "golden" server images and data backup to ensure that server images and data backups are undamaged/unbroken?

Classification - Internal

15(h)(vii)	RC.RP.S1	In case of ransomware attacks that specifically target backups, does the RE create backups in an isolated and immutable (and/or air-gapped) manner to ensure recovery if the production system is compromised?
15(h)(viii)	RC.RP.S1	Has the RE undertake regular business continuity drills to check the readiness of the organization and effectiveness of existing security controls at the ground level? Does the RE test recovering from a ransomware attack considering both PDC and DRS have been impacted to assess the effectiveness of people, processes, and technologies to deal with such attacks?
15(i)	RC.RP.S2	In the event of disruption of any one or more of the critical systems, Does the REs has designed and tested its systems and processes to enable the safe resumption of critical operations within two hours of a disruption, even in the case of extreme but plausible scenarios. Does the REs systems has capability to resume critical operations within two hours(i.e. RTO) and while dealing with a disruption REs have exercise judgment in effecting resumption so that risks to itself or its ecosystem do not thereby escalate. In consultation with their IT Committee, Does the REs have also plan for scenarios in which the resumption objective is not achieved? Does REs have RPO of 15 minutes for critical systems as per SEBI Circular issued from time to time.
15(i)(i)	RC.RP.S2	Does the RE conduct comprehensive scenario-based cyber resilience testing at least 2 times in a financial year (periodicity of such testing shall be of 6 months), to validate their ability to recover and resume operations following a cybersecurity incident/attack within prescribed RTO and RPO defined by SEBI CSCRF? In this regard, does the RE incorporate extreme plausible cyberattack scenarios into their cyber response and recovery planning? Are the said scenarios devised by the REs in consultation with their respective IT Committee for REs based on the learning from various sources such as past cybersecurity incidents, near-miss analysis, data from Security Operations Centre, honeypot logs analysis, etc.?
15(i)(ii)	RC.RP.S2	Does the RE periodically conduct backup testing and restore back-up data to check its usability?
15(i)(iii)	RC.RP.S2	For cyber resilience testing, does the RE also include stakeholders such as critical third-party service providers, market intermediaries, linked REs, etc.?

Classification - Internal

15(j)	RC.RP.S3	Does the RE conduct suitable periodic drills to test the adequacy and effectiveness of the response and recovery plan?
15(k)	RC.RP.S4	1.Has the RE formulated a backup and recovery plan approved by their respective IT Committee for REs? 2.Does the backup and recovery plan include policies and software solutions that work together to maintain business continuity in the event of a security incident? 3.Does such a plan include guidance on restoration of data with the backup software used by the RE?
15(k)(i)	RC.RP.S4	Does the backup and recovery policy include backup of data as well as backup of server images?
15(k)(ii)	RC.RP.S4	Are the backups of data and server images maintained at off-site locations to keep backup copies intact and unbroken?
15(k)(iii)	RC.RP.S4	Are RTO and RPO, as prescribed by SEBI CSCRF from time to time, included in the recovery plan for the restoration of systems after cybersecurity incidents?
15(l)	RC.IM.S1	While ensuring the protection of data, and security of processes, do the RE's BCP-DR capabilities support its cyber resilience objectives, and rapid recovery and resumption of critical operations after a cybersecurity incident?
15(l)(i)	RC.IM.S1	Does the RE try to incorporate lessons learned from incidents reported (if any) by other REs?
15(m)	RC.IM.S2	Does the RE meet their RTO for all interconnected systems and networks through capacity upgradations and periodic coordinated resilience testing?
15(m)(i)	RC.IM.S2	Is the recovery plan improved after analyzing the learnings from periodic drills?
15(n)	RS.MA.S2	Does the RE prepare cyber playbooks? Has the RE created a knowledge database for all known adverse conditions and attacks?
15(o)	EV.ST.S1,EV.ST.S2,EV.ST.S3	Does the RE maintain extra capacity of IT assets for information storage, processing, or communications?
15(p)	RC.RP.S4	Does the RE maintain offline, encrypted backups of data and regularly test these backups at least on a quarterly basis to ensure confidentiality, integrity, and availability of data?
16	**Sharing of Information**	
16(a)	RS.CO.S1,RS.CO.S2,RS.CO.S3	Reporting of Cybersecurity Incidents Does the RE share Threat Intelligence data that is collected, processed, and analyzed to gain insights into the motives and behavior of the

Classification - Internal

		threat actor, target, attack pattern, etc., on the SEBI Incident Reporting portal?
16(a)(i)	RS.CO.S1,RS.CO.S2,RS.CO.S3	Does the RE report incidents to CERT-In in accordance with the guidelines/directions issued by CERT-In from time to time? Additionally, does the RE, whose systems have been identified as "Protected system" by NCIIPC, also report the incident to NCIIPC?
16(a)(ii)	RS.CO.S1,RS.CO.S2,RS.CO.S3	Does the RE submit quarterly reports containing information on cyberattacks, threats, cybersecurity incidents, and breaches experienced, along with measures taken to mitigate vulnerabilities, threats, and attacks, including information on bugs/vulnerabilities and threats that may be useful for other REs and SEBI, within 15 days from the quarter ended June, September, December, and March of every year?
16(a)(iii)	RS.CO.S1,RS.CO.S2,RS.CO.S3	Does the RE share details deemed useful for other REs in a masked manner using a mechanism specified by SEBI from time to time? While sharing sensitive information, does the RE follow TLP with four levels of sensitivity: white, green, amber, or red?
17	**Training and Education**	
17(a)	PR.AT.S1, PR.AT.S2	Does the RE work on building awareness of cybersecurity, cyber resilience, and system hygiene among employees (with a focus on employees from non-technical disciplines)?
17(a)(i)	PR.AT.S1, PR.AT.S2	Does the RE ensure that their employees are aware of potential risks including social engineering attacks, phishing, etc.?
17(a)(ii)	PR.AT.S1, PR.AT.S2	Has the RE established thoughtfully designed security awareness campaigns as an essential pillar of defense, stressing the avoidance of clicking on links and attachments in emails? Additionally, does RE refer to advisories issued by CERT-In/CSIRT-Fin for assistance in conducting exercises for public awareness?
17(a)(iii)	PR.AT.S1, PR.AT.S2	Does the RE conduct periodic training programs to enhance the knowledge of IT/cybersecurity policy and standards among employees, incorporating up-to-date cybersecurity threats? Where possible, is this extended to outsourced staff, third-party service providers, etc.?
17(a)(iv)	PR.AT.S1, PR.AT.S2	Does the RE review and update training programs to ensure that the contents remain current and relevant?
17(b)	PR.AT.S3	Does the RE improve and maintain customer/investor awareness and education with regard to cybersecurity risks?

Classification - Internal

17(b)(i)	PR.AT.S3	Does the RE encourage customers/investors to report phishing mails/phishing sites and take effective remedial action on such reporting?
17(b)(ii)	PR.AT.S3	Does the RE educate the customers/investors on the downside risk of sharing their login credentials/passwords/OTP etc. with any third-party and the consequences thereof?
17(c)	RS.MA.S2	In order to optimize the RE's ability to respond in a timely and appropriate manner, Does the RE create cybersecurity awareness? Does the RE provide cybersecurity training to the relevant teams? Does the RE develop or hire people with appropriate skill sets?
17(d)	ID.RA.S3	Has the RE subscribed to anti-phishing/anti-rogue app services to mitigate potential phishing or impersonation attacks?
18	**Systems managed by vendors**	
18(a)	GV.SC.S4	Where the systems (IBT, Back office and other customer facing applications, IT infrastructure, etc.) of a RE are managed by third-party service providers and in case the RE does not have direct control over the implementation of any of the guidelines, whether the RE has instructed the third-party service providers to adhere to the **applicable guidelines in the CSCRF** and has obtained the necessary cyber audit certifications from them to ensure compliance with the framework?
18(a)(i)	GV.SC.S4	Does the responsibility, accountability, and ownership of outsourced activities lie primarily with the RE? Does the RE come up with appropriate monitoring mechanisms through a clearly defined framework to ensure that all the requirements as specified in SEBI CSCRF shall be complied with? Do the periodic reports submitted to SEBI highlight the critical activities handled by the third-party service providers, and does the RE certify that the above-mentioned requirement is complied with?
18(a)(ii)	GV.SC.S4	Does the RE conduct background checks and ensure signing of Non-Disclosure Agreements and cybersecurity compliance for all third-party service providers?
18(b)	PR.DS.S6	i.Does the RE obtain the source codes for all critical applications from their third-party service providers? ii.Where obtaining the source code is not possible, has the RE put in place a source code escrow arrangement or other equivalent arrangements to adequately mitigate the risk of default by the third-party service provider? Does the RE ensure that all product updates and patches/fixes are included in the source code escrow arrangement? iii.For all the software and applications where

Classification - Internal

		vulnerabilities will be identified at a later date, does the RE ensure that the vulnerabilities are mitigated in a time-bound manner? Has the RE also stipulated timelines in their SLA with their third-party service providers for the timely compliance and closure of identified vulnerabilities? iv.Has the RE put in place appropriate third-party service providers (including software vendors), risk assessment processes, and controls proportionate to their criticality/risk, **Service Level Agreements (SLAs) and contractual obligations** in order to manage supply chain risks effectively, **Third-party service providers shall be mandated to follow similar or higher standards of information security?** v.Does the RE ensure that maintenance and necessary support for applications/software are provided by the third-party service providers (including software vendors) and that this is enforced through a formal agreement?
19	**SEBI and Exchange/Depositories Compliances, Advisory for Financial Sector Organizations**	
19(a)	GV.OC.S2	Does the RE understand, manage, and comply with relevant cybersecurity and data security/protection requirements mentioned in government guidelines/policies/laws/circulars/regulations, etc., issued by SEBI/GoI such as IT Act 2000, Digital Personal Data Protection Act (DPDP) 2023 or any other law/circular/regulation as and when issued?
19(a)(i)	GV.OC.S2	Does the RE conduct audits and inspections of IT resources of the RE (and its sub-contractors/third-party service providers) or engage third-party auditors to conduct the same and check the adherence with SEBI and government guidelines/policies/laws/circulars/regulations, etc., and standard industry practices?
19(a)(ii)	GV.OC.S2	Do the policy and procedures of the RE mention and support the following? SEBI/Any other government agency shall at any time perform search and seizure of the RE's IT resources storing/processing data and other relevant IT resources (including but not limited to logs, user details, etc.) pertaining to the RE. In this process, SEBI or SEBI-authorized personnel/agencies may access RE IT infrastructure, applications, data, documents, including other necessary information given to, stored, or processed by third-party service providers?

Classification - Internal

19(a)(iii)	GV.OC.S2	Do the policy and procedures of the RE mention and support the following: SEBI shall seek the audit reports of the audits conducted by RE?
19(b)	GV.PO.S1, GV.PO.S2, GV.PO.S5	Whether the RE's policy and procedures includes below clause? All information/ data (classified as Regulatory Data and IT and Cybersecurity Data) that is consumed/ handled by REs shall be made accessible to SEBI when required. If there is any dependency on external party, REs shall facilitate information sharing with SEBI by including it in their agreement with external party.
19 (c)	PR.AA.S8	Is a strong log retention policy implemented as per government guidelines/policies/laws/circulars/regulations, etc., issued by SEBI/GoI such as IT Act 2000, Digital Personal Data Protection Act (DPDP) 2023, and as required by CERT-In, NCIIPC or any other government agency?
19(d)	PR.DS.S1, PR.DS.S2, PR.DS.S3	Does the RE keep the Regulatory Data available and easily accessible in legible and usable form within the legal boundaries of India? For investors whose country of incorporation is outside India, does the RE keep the original data available and easily accessible in legible and usable form within the legal boundaries of India? Further, if the Regulatory Data retained within India is not in readable form, does the RE maintain an application/system to read/analyze the retained data?
19(d)(i)	PR.DS.S1, PR.DS.S2, PR.DS.S3	For SaaS-based cybersecurity solutions and SOC offerings utilized by the RE where the data is not processed/stored within the legal boundaries of India, is such data classified, assessed, and periodically reviewed (at least once in a year) by the respective IT Committee for REs or the equivalent body of the RE? Is such IT and cybersecurity data approved by the Board/Partners/Proprietor annually? Is such data made available to SEBI/CERT-In/any other government agency whenever required within a reasonable time not exceeding 48 hours from the time of request?
19(d)(ii)	PR.DS.S1, PR.DS.S2, PR.DS.S3	During data classification, does the RE adhere to data security standards and guidelines and other government guidelines/policies/laws/circulars/regulations, etc., issued by SEBI/GoI such as IT Act 2000, Digital Personal Data Protection Act (DPDP) 2023 or any other law/circular/regulation as and when issued?
19(d)(iii)	PR.DS.S1, PR.DS.S2, PR.DS.S3	For capacity planning and monitoring, does the RE comply with circulars/guidelines on capacity

Classification - Internal

		planning issued by SEBI (and updated from time to time)?
19 (e)	ID.RA.S3	Has the RE been onboarded to the CERT-In intelligence platform to receive the advisories for necessary action and implementation?
19(f)	GV.SC.S7	Does the RE comply with the SEBI circulars on outsourcing of activities, which are currently mandated and updated from time to time, as listed in SEBI CSCRF?
20	**Cyber Security Advisory - Standard Operating Procedure (SOP)**	
20(a)	RS.MA.S1	Cyber Security Advisory – Standard Operating Procedure (SOP) for handling cyber security incidents of intermediaries-as per SEBI directives. The aspects which shall form part of the SOP and whether stockbroker/depository participant has complied?
20(a)(i)	RS.MA.S1	Does members have a well-documented Cyber Security incident handling process document (Standard Operating Procedure - SOP) in place? Is the policy approved by Board of the Member (in case of corporate trading member), Partners (in case of partnership firms) or Proprietor (in case of sole proprietorship firm) as the case may be and be reviewed annually by the “Internal Technology Committee” as constituted under SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 for review of Security and Cyber Resilience policy?
20(a)(ii)	RS.MA.S1	Does member examine the Cyber Security incident and classify the Cyber Security incidents into High/ Medium/ Low as per their Cyber Security incident handling process document? Does the Cyber Security incident handling process document define decision on Action/ Response for the Cyber Security incident based on severity?
20(b)	RS.CO.S1, RS.CO.S2, RS.CO.S3	Have members reported the Cyber Security incident to Indian Computer Emergency Response Team (CERT-In)?
20 (c)	RS.CO.S1, RS.CO.S2, RS.CO.S3	Have members provided the reference details of the reported Cyber Security incident with CERT-In to the Exchange and SEBI? Have members also provided details, regarding whether CERT-In team is in touch with the Member for any assistance on the reported Cyber Security incident? If the Cyber Security incident is not reported to CERT-In, have members submitted the reasons for the same to the Exchange/depositories and SEBI? Have members communicated with CERT-In/ Ministry of Home Affairs (MHA)/ Cyber Security Cell of Police for further assistance on the reported Cyber Security incident?

Classification - Internal

20(d)	ID.RA.S3	Has the RE devised SOPs to implement the advisories issued by CERT-In, NCIIPC or any other government agency in their IT environment within a defined timeframe?
21	**Security of Cloud Services:**	
21(a)	21(a)	Does the RE check the public accessibility of all cloud instances in use to ensure that no server or bucket is inadvertently leaking data due to inappropriate configurations?
21(b)	21(b)	Are the tokens exposed publicly in website source code, any configuration files etc.?
21 (c)	21(C)	Has the RE implemented appropriate security measures for testing, staging, and backup environments hosted on the cloud? Has the RE ensured that the production environment is properly segregated from these environments? Additionally, has the RE disabled or removed older or testing environments if their usage is no longer required?
21(d)	21(d)	Has the RE considered employing hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments?
21 (e)	21 (e)	Ensure alignment with Governance, Risk, and Compliance (GRC) standards within cloud computing operations and practices. Refer principle 1 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023.
21(f)	21(f)	Ensure compliance with established guidelines and protocols in the selection and engagement of cloud service providers. Refer principle 2 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023.
21(g)	21(g)	Ensure compliance with data ownership and localization requirements as mandated by relevant regulations and policies within cloud operations. Refer principle 3 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023.
21(h)	21(h)	Ensure that the RE assumes responsibility for maintaining compliance with all relevant cloud computing regulations and standards. Refer principle 4 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023.
21(i)	21(i)	Ensure that the RE conducts thorough due diligence when assessing cloud service providers and their compliance with regulatory requirements. Refer principle 5 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023.

Classification - Internal

21(j)	21(j)	Is robust security controls implemented and maintained to safeguard data and systems in compliance with cloud computing regulations and standards. Refer principle 6 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023?
21(k)	21(k)	Ensure that contractual agreements with cloud service providers align with regulatory obligations to maintain compliance within cloud operations. Refer principle 7 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023.
21(l)	21(l)	Are Business Continuity Planning (BCP), Disaster Recovery, and Cyber Resilience measures integrated into cloud operations to ensure compliance with regulatory requirements. Refer principle 8 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023?
21(m)	21(m)	Are strategies implemented to manage vendor lock-in and concentration risks effectively in cloud operations to maintain compliance with regulatory standards. Refer principle 9 of SEBI circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 Dated March 06, 2023?
21(n)	PR.IP.S15	Software services in the form of SaaS/hosted services used by RE: 1.Does the RE submit compliance with the technical specifications mentioned in the hosted services definition for the SaaS/hosted services used by them? 2.Does the RE also submit compliance with the adoption of hosted services and SaaS as per the various functions of CSCRF, including Governance, Identify, Protect, Detect, Respond, and Recover?
22	**Concentration Risk on Outsourced Agencies:**	
22(a)	GV.SC.S7	Whether the RE has taken into account concentration risk (where single third-party vendors provide services to multiple REs) while outsourcing multiple critical services to the same vendor?
22(a)(i)	GV.SC.S7	Whether the organization has identified third-party service providers posing a concentration risk and prescribe specific cybersecurity controls, including audits of their systems and protocols by independent auditors, to mitigate such risks, and does the organization validate that these third-party service providers are meeting their goals of operational resiliency?
23	**Certification of off-the-shelf products**	

Classification - Internal

23(a)	PR.IP.S15	Customized COTS: Does the RE ensure that compliance with the tests/audits stated below is met by CERT-In empanelled IS auditing organizations for any customized COTS? a Application security testing: i. Dynamic Application Security Testing (DAST) for scanning software applications in real-time against leading vulnerability sources, such as OWASP Top 10, SANS Top 25 CWE, etc. to find security flaws or open vulnerabilities ii. Static Application Security Testing (SAST) for analyzing program source code to identify security vulnerabilities such as SQL injection, buffer overflows, XML external entity (XXE) attacks, OWASP Top 10 security risks, etc. b. Functional audit c. VAPT after every major release of the application/software d. All critical systems logs integrated with the RE's SOC by CERT-In empanelled IS auditing organizations for any customized COTS
23(a)(i)	PR.IP.S15	Inhouse developed software: Does the RE ensure that compliance with the below points is submitted by CERT-In empanelled IS auditing organizations? 1. All the categories of software solutions/applications/products for critical systems used by REs shall mandatorily pass-through the following tests/audits and compliances: a. Application security testing: i. Dynamic Application Security Testing (DAST) for scanning software applications in real-time against leading vulnerability sources, such as OWASP Top 10, SANS Top 25 CWE, etc. to find security flaws or open vulnerabilities. ii. Static Application Security Testing (SAST) for analyzing program source code to identify security vulnerabilities such as SQL injection, buffer overflows, XML external entity (XXE) attacks, OWASP Top 10 security risks, etc. b. Functional audit c. VAPT after every major release of the application/software d. All critical systems logs shall be integrated with RE's SOC. e. Audit of firewall configuration, WAF configuration, token configuration and channel identification shall be done. f. Software Bill of Material (SBOM) g. Requirement Traceability Matrix
24	**Compliance status of last inspection carried out by SEBI/ Depository**	

Classification - Internal

24(a)		Has Member taken corrective steps to rectify the deficiencies observed in the inspection carried out by SEBI? Further, whether Member has complied with the qualifications/violations made in last SEBI inspection report?
24(b)		Has Member taken corrective steps to rectify the deficiencies observed in the inspection carried out by Depository? Further, has Member complied with the qualifications/violations made in last Member inspection report?

Internal

Classification - Internal

This is to be submitted by the RE

Annexure C

Cyber Audit Report Format

Cyber audit report format for compliance submission

NAME OF THE ORGANISATION: <Name>

ENTITY TYPE: <Intermediary Type>

ENTITY CATEGORY: <Category of the RE as per CSCRF>

RATIONALE FOR THE CATEGORY: <>

PERIOD OF AUDIT: <>

NAME OF THE AUDITING ORGANISATION: <Name>

Date on Which Cyber Audit Report presented to 'IT Committee for REs' : <Date>

RE's Authorised signatory declaration:

I/ We hereby confirm that the information provided herein is verified by me/ us and I/ we shall take the responsibility and ownership of this cyber audit report.

Further, this is to certify that:

a. Comprehensive measures and processes including suitable incentive/ disincentive structures, have been put in place for identification/ detection and closure of vulnerabilities in the organization's IT systems.

b. Adequate resources have been hired for staffing our Security Operations Centre (SOC).

c. There is compliance by us with CSCRF.

Signature:

Name of the signatory:

Designation (choose whichever applicable): <MD/ CEO/ Board member/ Partners/ Proprietor>

Company stamp:

Annexures:

1. Minutes of the Meeting (MoM) of 'IT Committee for REs' <Date> in which the cyber audit report was approved.

2. Cyber audit report as submitted by the auditor

Classification - Internal

This is to be submitted by the auditor on the Auditors letter head.

1. Auditor's Declaration

TO WHOM SO EVER IT MAY CONCERN

This is to declare and certify that I am a Partner/Proprietor of firm <Name of the Auditing Organization> with CERT-In empanelment from <Date> to <Date>. I have conducted Cyber audit for <Name of the RE> period <….> as per the requirements of SEBI.

Checklist for Cyber audit as required:

Sr. No	Area	Details of the audit area	Is the Entity Compliant? (Yes/No)	Auditor's comments
1.	Cybersecurity and Cyber resilience policy			
2.	Asset Inventory			
3.	Risk assessment and Risk management			
4.	Supply chain risk management			
5.	Awareness and Training			
6.	Data security			
7.	Security continuous monitoring			
8.	SOC efficacy			
9.	Incident Management and Response			
10.	Incident recovery planning			

I confirm that the audit has been conducted as per the auditor's guidelines prescribed in CSCRF (Cyber Audit).

I also confirm that I have no conflict of interest in undertaking the above-mentioned audit.

For and on behalf of

Name:

Contact no.:

Place:

Date:

Classification - Internal

2. Executive Summary

<Auditing Organization to provide an executive summary of the findings>

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

3.1. List of SEBI Circulars/ Guidelines/ Advisories/ Letters covered:

S. No.	SEBI circular/ letter/ advisory	Issue date

3.2. List of all IT infrastructure and geographical locations (including IT systems of PDC, DR, Near site, Co-lo facility) covered under audit

S. No.	List of IT infrastructure/ Geographical locations/ Third-party vendors	Details (assets ID, asset name, applications, etc.) of the Infrastructure assessed
1.	PDC	
2.	DR	
3.	Near-site	
4.	Co-location Facility (if applicable)	
5.	Cloud Infrastructure	
6.	Third-party service provider	
7.	Others	

3.3. Any other specific item(s) :

4. Methodology/ Audit approach (audit subject identification, pre-audit planning, data gathering methodology, sampling methodology etc. followed by the Auditing Organization)

5. Summary of findings (including identification tests, tools used, and results of tests performed)

S. No	Number of Non-Compliant/Observation	Risk rating				Any other comments
		Critical	High	Medium	Low	

Classification - Internal

6. Detailed Control-wise compliance report & status of SEBI CSCRF will upload detailed report in excel file as per format provided by the exchange/depository.

S.No	Standards prescribed by SEBI CSCRF (Clause number and text)	Description of Finding(s)/ Observation(s)	Name of the system belongs to RE or third-party vendor	Status/nature of findings	Risk rating (C/H/M/L) of the findings	C/I/A affected	Test cases used	Root Cause Analysis	Impact analysis	Auditor recommendations/ Corrective actions	Deadline of corrective action(s)	Management response	Whether similar issue was reported in the last three audits.	*List of documentary evidence including physical inspection/ sample size taken by the auditor
1	GV.OC.S1													
2	GV.OC.S2													
…														
N	EV.ST.S5													

Note: -

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

* Explicitly mention sample size and sample methodology covering 25% of the non-critical systems

7. **A brief description of the above-mentioned compliance requirements is as follows-**

i. Standards prescribed by SEBI CSCRF (or any other cybersecurity circular/ letter/ guidelines) (Clause number and text)- The clause corresponding to this observation w.r.t CSCRF (or any other cybersecurity circular/ letter/ guidelines) issued by SEBI.

ii. Description of findings/observations – Description of the findings in sufficient details, referencing any accompanying evidence

iii. Name of system belongs to RE or vendor - (Self Explanatory term)

iv. Status/ Nature of Findings – The category can be specified, for ex: Compliant, Non-Compliant, and Not Applicable

v. Risk Rating of the finding - A rating shall be given by the auditing organization 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
CRITICAL	The failure shall have impact on the system-delivery resulting in outage of services offered by the RE.
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 within a 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.

Classification - Internal

vi. C/I/A Affected **–** The principles of Confidentiality/ integrity/ availability affected due to issued left unaddressed**.**

vii. Test cases used **–**The details of test cases used for arriving at this observation. The test cases may also be provided as annexures with the report, if required.

viii. Root Cause analysis – A detailed analysis on the cause of the non-conformity.

ix. Impact Analysis **–** An analysis of the likely impact on the operations/ activity of the RE.

x. Auditor recommendations/ Corrective actions **–** The actions to be taken (by the RE) to correct the non-conformity.

xi. Deadline of corrective action(s) **-**The RE shall specify the deadline not only for the corrective action(s) to be taken on the system(s) where NC/ observation was found but also specify the deadline for corrective action on systems with related functionalities/ configurations where similar observations could have been found/are found.

xii. Management response – Management action plan/taken to address the observation and/ or implementation of auditor's recommendation

xiii. Whether similar issue was reported in the last three audits – Yes/ No

xiv. List of documentary evidence including physical inspection/ sample size taken by the auditor

8. Conclusion of cyber audit

****

Classification - Internal