Annexure A

Section	Sub Section	Area of Verification
1		**Governance**
1	A (i)	Whether the Stockbroker has formulated a comprehensive Cyber Security and Cyber Resilience policy document encompassing the framework mentioned in the circular?
	A (ii)	In case of deviations from the suggested framework, whether reasons for such deviations, technical or otherwise, are provided in the policy document?
	A (iii)	Is the policy document approved by the Board / Partners / Proprietor of the organization?
	A (iv)	Whether the policy document is reviewed by the aforementioned group at least annually with the view to strengthen and improve its Cyber Security and Cyber Resilience framework.
	A (v)	Policy Approval Date
	A (vi)	Policy Version
	A (vii)	Policy Approval By
1	B (i)	Whether the Cyber Security Policy includes the following process to identify, assess, and manage Cyber Security risk associated with processes, information, networks, and systems:
	B (ii)	a. 'Identify' critical IT assets and risks associated with such assets.
	B (iii)	b. 'Protect' assets by deploying suitable controls, tools, and measures.
	B (iv)	c. 'Detect' incidents, anomalies, and attacks through appropriate monitoring tools/processes.
	B (v)	d. 'Respond' by taking immediate steps after identification of the incident, anomaly, or attack.
	B (vi)	e. 'Recover' from incident through incident management and other appropriate recovery mechanisms.
1	C	Whether policy / Procedure document refers to best practices from international standards like ISO 27001, COBIT 5, etc., or their subsequent revisions, if any, from time to time.
1	D	Whether policy document have considered the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organization (NTRO), Government of India (titled 'Guidelines for Protection of National Critical Information Infrastructure') and subsequent revisions, if any, from time to time.

Section	Sub Section	Area of Verification
1	E	Stockbrokers / Depository Participants should designate a senior official or management personnel (henceforth, referred to as the "Designated Officer") whose function would be to assess, identify, and reduce security and Cyber Security risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the Cyber Security Policy.
1	F (i)	Whether the Member has constituted an Technology Committee comprising experts.
	F (ii)	This Technology Committee has reviewed on a half yearly basis the implementation of the Cyber Security and Cyber Resilience policy, which includes:
	F (iii)	- review of their current IT and Cyber Security and Cyber Resilience capabilities,
	F (iv)	- if committee has set goals for a target level of Cyber Resilience and establish plans to improve and strengthen Cyber Security and Cyber Resilience.
	F (v)	- And the review report is placed before the Board / Partners / Proprietor of the Stockbrokers / Depository Participants for appropriate action.
1	G	Whether the Designated officer and the technology committee periodically reviewed instances of cyber-attacks, if any, domestically and globally, and taken steps to strengthen Cyber Security and cyber resilience framework.
1	H	Whether Brokers / Depository Participants has policy or reporting procedure to facilitate communication of unusual activities and events to the Designated Officer in a timely manner.
1	I	Has Stockbroker/Depository Participant defined and documented roles and responsibilities of its employees, outsourced staff, and employees of vendors, members or participants and other entities, who may have privileged access or use systems / networks of the Stockbroker/Depository Participants towards ensuring the goal of Cyber Security?
1	J	Stockbrokers / Depository Participants should prepare detailed incident response plan and define roles and responsibilities of Chief Information Security Officer (CISO) and other senior personnel. Reporting and compliance requirements shall be clearly specified in the security policy. In addition, share the details of CISO with CERT-In through Email (info AT cert-in.org.in)
2		**Identification**

Section	Sub Section	Area of Verification
2	A	Has the Stock Broker / Depository Participant identified and classified critical assets based on their sensitivity and criticality for business operations, services and data management. The critical assets shall include business critical systems, internet facing applications /systems, systems that contain sensitive data, sensitive personal data, sensitive financial data, Personally Identifiable Information (PII) data, etc. All the ancillary systems used for accessing/communicating with critical systems either for operations or maintenance shall also be classified as critical system. The Board/Partners/Proprietor of the Stock Brokers / Depository Participants shall approve the list of critical systems. To this end, Stock Brokers / Depository Participants should maintain up-to-date inventory of its hardware and systems and the personnel to whom these have been issued, software and information assets (internal and external), details of its network resources, connections to its network and data flows.
2	B	Has the Stockbrokers / Depository Participants identified / has process to identify cyber risks (threats and vulnerabilities) that it may face, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.
3		**Protection**
3	A	Access control No person by virtue of rank or position should have any intrinsic right to access Confidential data, applications, system resources or facilities.
3	B	Any and all access to Stockbrokers / Depository Participants systems, applications, networks, databases etc., have defined purpose and for a defined period. Stockbrokers / Depository Participants should grant access to IT systems, applications, databases, and networks on a need-to-use basis and based on the principle of least privilege to provide security for both on-and off-premises resources (i.e. zero-trust models). Such access should be for the period when the access is required and should be authorized using strong authentication mechanisms.
3	C	Have Stockbrokers / Depository Participants implemented an access policy which addresses strong password controls for users' access to systems, applications, networks, and databases. Illustrative examples for this are given in Annexure C of SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018
3	D	All critical systems of the Stockbroker / Depository Participant accessible over the internet should have two-factor security (such as VPNs, Firewall controls etc.)
3	E	Stockbrokers / Depository Participants should ensure that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes. Such logs should be maintained and stored in a secure location for a time period not less than two (2) years.

Section	Sub Section	Area of Verification
3	F	Stockbrokers / Depository Participants should deploy controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users) to Stockbroker / Depository Participant's critical systems. Such controls and measures should inter-alia include restricting the number of privileged users, periodic review of privileged users' activities, disallow privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.
3	G	Employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to the Stockbrokers / Depository Participants critical systems, networks, and other computer resources, should be subject to stringent supervision, monitoring, and access restrictions.
3	H	Stockbrokers / Depository Participants should formulate an Internet access policy to monitor and regulate the use of internet and internet-based services such as social media sites, cloud-based internet storage sites, etc. within the Stockbroker / Depository Participant's critical IT infrastructure.
3	I	User Management must address deactivation of access of privileges of users who are leaving the organization or whose access privileges have been withdrawn.
4		**Physical Security**
4	A	Physical access to the critical systems should be restricted to minimum and only to authorized officials. Physical access of outsourced staff/visitors should be properly supervised by ensuring at the minimum that outsourced staff/visitors are always accompanied by authorized employees.
4	B	Physical access to the critical systems should be revoked immediately if the same is no longer required.
4	C	Stockbrokers/ Depository Participants has ensured that the perimeter of the critical equipment's room, if any, are physically secured and monitored by employing physical, human, and procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. where appropriate
5		**Network Security Management**
5	A	Stockbrokers / Depository Participants has established baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within their IT environment.
5	B	The LAN and wireless networks should be secured within the Stockbrokers /Depository Participants' premises with proper access controls.

Section	Sub Section	Area of Verification
5	C	For algorithmic trading facilities, adequate measures should be taken to isolate and secure the perimeter and connectivity to the servers running algorithmic trading applications.
5	D	Stockbrokers / Depository Participants should install network security devices, such as firewalls, proxy servers, intrusion detection and prevention systems (IDS) to protect their IT infrastructure which is exposed to the internet, from security exposures originating from internal and external sources.
5	E	Adequate controls must be deployed to address virus / malware / ransomware attacks. These controls may include host / network / application-based IDS systems, customized kernels for Linux, anti-virus, and anti-malware software etc.
6		**Data security**
6	A	Critical data must be identified and encrypted in motion and at rest by using strong encryption methods. Illustrative measures in this regard are given in Annexure A and B of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018
6	B	Stockbrokers / Depository Participants should implement measures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity. It should be ensured that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties. Illustrative measures to ensure security during transportation of data over the internet are given in Annexure B of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018
6	C	The information security policy should also cover use of devices such as mobile phones, faxes, photocopiers, scanners, etc., within their critical IT infrastructure, that can be used for capturing and transmission of sensitive data. For instance, defining access policies for personnel, and network connectivity for such devices etc.
6	D	Stockbrokers / Depository Participants should allow only authorized data storage devices within their IT infrastructure through appropriate validation processes.
6	E	Stockbrokers / Depository Participants should Enforce BYOD (Bring your own device) security policies, like requiring all devices to use a business-grade VPN service and antivirus protection
6	F	Stockbrokers/ Depository Participants shall deploy detection and alerting tools. Members shall create process to prevent, contain and respond to a data breach/ data leak.
7		**Hardening of Hardware and Software**

Section	Sub Section	Area of Verification
7	A	Whether Member only deploys hardened hardware / software, including replacing default passwords with strong passwords and disabling or removing services identified as unnecessary for the functioning of the system.
7	B	Whether Open ports on networks and systems which are not in use or that can be potentially used for exploitation of data should be blocked and measures taken to secure them.
8		**Application Security in Customer Facing Applications**
8	A	Whether over the Internet application like IBTs (Internet Based Trading applications) portal and back-office application, containing sensitive or private information are secured by using security measures. (Illustrative list of measures for ensuring security in such applications is provided in Annexure C of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018
9		**Certification of off-the-shelf products**
9	A	Stockbrokers / Depository Participants should ensure that off the shelf products being used for core business functionality (such as Back-office applications) should 1. bear Indian Common criteria certification of Evaluation Assurance Level 4. The Common criteria certification in India is being provided by (STQC) Standardisation Testing and Quality Certification (Ministry of Electronics and Information Technology). or 2. Certified independently on criteria similar to Indian Common Criteria Certificate of Evaluation Assurance Level. Custom developed / in-house software and components need not obtain the certification, but must undergo intensive regression testing, configuration testing etc. The scope of tests should include business logic and security controls.
10		**Patch management**
10	A	Stockbrokers / Depository Participants should establish and ensure that the patch management procedures include the identification, categorization and prioritization of patches and updates. An implementation timeframe for each category of patches should be established to apply them in a timely manner.
10	B	Stockbrokers / Depository Participants should perform rigorous testing of security patches and updates, where possible, before deployment into the production environment to ensure that the application of patches do not impact other systems.
11		**Disposal of data, systems, and storage devices**
11	A	Stockbrokers / Depository Participants should frame suitable policy for disposal of storage media and systems. The critical data / Information on such devices and systems should be removed by using methods such as crypto shredding / degauss / Physical destruction as applicable.

Section	Sub Section	Area of Verification
11	B	Stockbrokers / Depository Participants should formulate a data-disposal and data-retention policy to identify the value and lifetime of various parcels of data.
12		**Vulnerability Assessment and Penetration Testing (VAPT)**
12	A	Stock Brokers / Depository Participants shall carry out periodic Vulnerability Assessment and Penetration Tests (VAPT) which inter-alia include critical assets and infrastructure components like Servers, Networking systems, Security devices, load balancers, other IT systems pertaining to the activities done as Stock Brokers / Depository Participants etc., in order to detect security vulnerabilities in the IT environment and in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks
12	B	Stock Brokers / Depository Participants shall conduct VAPT at least once in a financial year. All Stock Brokers / Depository Participants are required to engage only CERT-In empanelled organizations for conducting VAPT. The final report on said VAPT shall be submitted to the Stock Exchanges / Depositories after approval from Technology Committee of respective Stock Brokers / Depository Participants, within 1 month of completion of VAPT activity.
12	C	In addition, Stock Brokers / Depository Participants shall perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system which is a critical system or part of an existing critical system.
12	D	In case of vulnerabilities discovered in off-the-shelf products (used for core business) or applications provided by exchange empanelled vendors, Stockbrokers / Depository Participants should report them to the vendors and the exchanges in a timely manner.
12	E	Any gaps/vulnerabilities detected shall be remedied on immediate basis and compliance of closure of findings identified during VAPT shall be submitted to the Stock Exchanges / Depositories within 3 months post the submission of final VAPT report
13		**Monitoring and Detection**
13	A	Stockbrokers / Depository Participants should establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events / alerts and timely detection of unauthorised or malicious activities, unauthorised changes, unauthorised access and unauthorised copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices exposed to the internet should also be monitored for anomalies.

Section	Sub Section	Area of Verification
13	B	Further, to ensure high resilience, high availability, and timely detection of attacks on systems and networks exposed to the internet, Stockbrokers / Depository Participants should implement suitable mechanisms to monitor capacity utilization of its critical systems and networks that are exposed to the internet, for example, controls such as firewalls to monitor bandwidth usage.
14		**Response and Recovery**
14	A	Alerts generated from monitoring and detection systems should be suitably investigated to determine activities that are to be performed to prevent expansion of such incident of cyber-attack or breach, mitigate its effect, and eradicate the incident.
14	B	The response and recovery plan of the Stockbrokers / Depository Participants should have plans for the timely restoration of systems affected by incidents of cyber-attacks or breaches, for instance, offering alternate services or systems to Customers. Stockbrokers / Depository Participants should have the same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as specified by SEBI for Market Infrastructure Institutions vide SEBI circular CIR/MRD/DMS/17/20 dated June 22, 2012 as amended from time to time
14	C	The response plan should define responsibilities and actions to be performed by its employees and support / outsourced staff in the event of cyber-attacks or breach of Cyber Security mechanism.
14	D	Any incident of loss or destruction of data or systems should be thoroughly analysed
14	E	And lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes.
14	F	Stockbrokers / Depository Participants should also conduct suitable periodic drills to test the adequacy and effectiveness of the response and recovery plan.
15		**Sharing of Information**
15	A	All Cyber-attacks, threats, cyber-incidents and breaches experienced by Stock Brokers / Depositories Participants shall be reported to Stock Exchanges / Depositories /CERT-IN & SEBI within 6 hours of noticing / detecting such incidents or being brought to notice about such incidents. This information shall be shared to SEBI through the dedicated e-mail id: incident@cert-in.org.in & sbdp-cyberincidents@sebi.gov.in.

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

Section	Sub Section	Area of Verification
18	B	1- Adherence to all such Circulars, Notices, Guidelines, and advisories published
18	C	2- Reporting adherences based on prescribed periodicity in point 1 above
19		**Advisory for Financial Sector Organizations:**
19	A	Whether compliance of the SEBI circular no. SEBI/HO/MIRSD2/DOR/CIR/P/ 2020/221 dated November 03, 2020, for Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions has been made.
20		**Cyber Security Advisory - Standard Operating Procedure (SOP)**
20	A	Cyber Security Advisory – Standard Operating Procedure (SOP) for handling cyber security incidents of intermediaries-as per SEBI directives. The aspects which shall form part of the SOP and whether stock-broker has to complied.
20	B	Members shall have a well-documented Cyber Security incident handling process document (Standard Operating Procedure - SOP) in place. Such policy shall be approved by Board of the Member (in case of corporate trading member), Partners (in case of partnership firms) or Proprietor (in case of sole proprietorship firm) as the case may be and shall be reviewed annually by the "Internal Technology Committee" as constituted under SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 for review of Security and Cyber Resilience policy.
20	C	Members shall examine the Cyber Security incident and classify the Cyber Security incidents into High/ Medium/ Low as per their Cyber Security incident handling process document. The Cyber Security incident handling process document shall define decision on Action/ Response for the Cyber Security incident based on severity.
20	D	Members shall report the Cyber Security incident to Indian Computer Emergency Response Team (CERT-In).
20	E	Members shall provide the reference details of the reported Cyber Security incident with CERTI n to the Exchange and SEBI. Members shall also provide details, regarding whether CERT-In team is in touch with the Member for any assistance on the reported Cyber Security incident. If the Cyber Security incident is not reported to CERT-In, members shall submit the reasons for the same to the Exchange and SEBI. Members shall communicate with CERT-In/ Ministry of Home Affairs (MHA)/ Cyber Security Cell of Police for further assistance on the reported Cyber Security incident.
20	F	Members shall submit details whether Cyber Security incident has been registered as a complaint with law enforcement agencies such as Police or its Cyber Security cell. If yes, details need to be provided to Exchange and SEBI. If no, then the reason for not registering complaint shall also be provided to Exchange and SEBI.

Section	Sub Section	Area of Verification
20	G	The details of the reported Cyber Security incident and submission to various agencies by the Members shall also be submitted to Division Chiefs (in-charge of divisions at the time of submission) of DOS-MIRSD and CISO of SEBI
20	H	The Designated Officer of the Member (appointed in terms of para 6 of the aforementioned SEBI Circular dated December 03, 2018) shall continue to report any unusual activities and events within 6 hours of receipt of such Information as well as submit the quarterly report on the cyber-attacks & threats within 15 days after the end of the respective quarter in the manner as specified in Exchange circular.
21		**TECHNICAL GLITCH**
21	A	Member has reported all instances of technical glitches within the prescribed timelines during the audit period in accordance with regulatory guidelines. Member has correctly reported the issues faced and duration of the downtime. Member has implemented all the measures as mentioned in RCAs and has taken necessary steps to prevent the recurrence of such technical glitch.