Cyber Security and Cyber Resilience Audit Terms of Reference (ToR)

Audit TOR Clause	Assessment Details
1	**Governance**
a	Whether the Stock Brker has formulated a comprehensive Cyber Security and Cyber Resilience policy document encompassing the framework mentioned in the circular? In case of deviations from the suggested framework, whether reasons for such deviations, technical or otherwise, are provided in the policy document? Is the policy document approved by the Board / Partners / Proprietor of the organization? 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.
b	The Cyber Security Policy should includes the following process to identify, assess, and manage Cyber Security risk associated with processes, information, networks and systems: a. 'Identify' critical IT assets and risks associated with such assets. b. 'Protect' assets by deploying suitable controls, tools and measures. c. 'Detect' incidents, anomalies and attacks through appropriate monitoring tools/processes. d. 'Respond' by taking immediate steps after identification of the incident, anomaly or attack. e. 'Recover' from incident through incident management and other appropriate recovery mechanisms.
c	The Cyber Security Policy of Stock Brokers trading through APIs based terminal / Depository Participants should consider 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.

d	Stock Brokers trading through APIs based terminal / Depository Participants may refer to best practices from international standards like ISO 27001, COBIT 5, etc., or their subsequent revisions, if any, from time to time.
e	Stock Brokers / 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.
f	Has the Board / Partners / Proprietor of the Stock Broker formed an internal Technology Committee comprising experts. This Technology Committee should on a half yearly basis review the implementation of the Cyber Security and Cyber Resilience policy approved by their Board / Partners / Proprietor, and such review should include review of their current IT and Cyber Security and Cyber Resilience capabilities, set goals for a target level of Cyber Resilience, and establish plans to improve and strengthen Cyber Security and Cyber Resilience. The review shall be placed before the Board / Partners / Proprietor of the Stock Brokers /Depository Participants for appropriate action
g	The Organization should establish a reporting procedure to facilitate communication of unusual activities and events to the Designated Officer in a timely manner.
h	Does the designated officer and technology committee periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen Cyber Security and cyber resilience framework?
i	Stock Broker/Depository Participant should define and document 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 Stock Broker/Depository Participants towards ensuring the goal of Cyber Security ?
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**

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.
b	Stock Brokers / Depository Participants should accordingly 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**
I	**Access Control**
a	Any and all accesses to Stock Brokers / Depository Participants systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period. Stock Brokers / 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. Such access should be for the period when the access is required and should be authorized using strong authentication mechanisms.
b	Stock Brokers / Depository Participants should implement 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
c	All critical systems of the Stock Broker / Depository Participant accessible over the internet should have two-factor security (such as VPNs, Firewall controls etc.)
d	Stock Brokers / 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.

e	Stock Brokers / Depository Participants should deploy controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users) to Stock Broker / 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.
f	Employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to the Stock Brokers / Depository Participants critical systems, networks and other computer resources, should be subject to stringent supervision, monitoring and access restrictions.
g	Stock Brokers / 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 Stock Broker / Depository Participant's critical IT infrastructure.
h	User Management must address deactivation of access of privileges of users who are leaving the organization or whose access privileges have been withdrawn.
i	Are there any users / person by virtue of rank or position that have any intrinsic right to access confidential data, applications, system resources or facilities. Do stockbrokers/Depository Participants use models that take the `least privilege' approach to provide security for both on-and off-premises resources (i.e. zero-trust models).
II	**Physical Security**
j	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 accompanied at all times by authorized employees.
k	Physical access to the critical systems should be revoked immediately if the same is no longer required.
l	Stock Brokers/ Depository Participants has ensured that the perimeter of the critical equipments 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
III	**Network Security Management**
m	Stock Brokers / 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.

n	The LAN and wireless networks should be secured within the Stock Brokers /Depository Participants' premises with proper access controls (Physical and Logical).
0	For algorithmic trading facilities, adequate measures should be taken to isolate and secure the perimeter and connectivity to the servers running algorithmic trading applications.
p	Stock Brokers / 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.
q	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.
IV	**Data Security**
r	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
s	Stock Brokers / 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
t	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.
u	Stock Brokers / Depository Participants should allow only authorized data storage devices within their IT infrastructure through appropriate validation processes.
v	Stock Brokers / Depository Participants should only deploy hardened hardware / software, including replacing default passwords with strong passwords and disabling or removing services identified as unnecessary for the functioning of the system.
w	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.

x	Stockbrokers/ Depository Participants shall deploy detection and alerting tools. Members shall create process to prevent, contain and respond to a data breach/ data leak.
y	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
V	**Application Security in Customer Facing Applications**
z	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 (repository of financial and personal information offered by Brokers to Customers) are secured by security measures. An 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 03 December 2018
VI	**Certification of off-the-shelf products**
aa	Stock Brokers / Depository Participants should ensure that off the shelf products being used for core business functionality (such as Back office applications) should 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).
ab	Custom developed / in-house software and components need not obtain the certification. Are the custom developed / in-house software and components undergone intensive regression testing, configuration testing etc. Does the scope of tests include business logic and security controls.
VI	**Patch management**
ac	Stock Brokers / Depository Participants should establish and ensure that the patch management procedures for software, hardware and applications (such as including Servers, OS, Database, Middleware, Network Devices, Firewalls, IDS /IPS Desktops etc.) include the identification, categorization and prioritization of applicable versions of patches and updates. An implementation timeframe for each category of patches should be established to apply them in a timely manner.
ad	Stock Brokers / Depository Participants should perform rigorous testing of security patches and updates, where possible, before deployment into the production environment so as to ensure that the application of patches do not impact other systems.
VII	**Disposal of data, systems and storage devices**

ae	Stock Brokers / 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.
af	Stock Brokers / Depository Participants should formulate a data-disposal and data-retention policy to identify the value and lifetime of various parcels of data.
VIII	**Vulnerability Assessment and Penetration Testing (VAPT)**
ag	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
ah	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 empaneled organizations for conducting VAPT. The final report on said VAPT shall be submitted to the Stock Exchanges / Depositories after approval from Technology Committee of respective Stock Brokers / Depository Participants, within 1 month of completion of VAPT activity.
ai	In case of vulnerabilities discovered in off-the-shelf products (used for core business) or applications provided by exchange empanelled vendors, Stock Brokers / Depository Participants should report them to the vendors and the exchanges in a timely manner.
aj	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
ak	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.
4	**Monitoring and Detection**

a	Stock Brokers / 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.
b	Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks exposed to the internet, Stock Brokers / 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.
5	**Response and Recovery**
a	Alerts generated from monitoring and detection systems should be suitably investigated in order 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.
b	The response and recovery plan of the Stock Brokers / 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. Stock Brokers / 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
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.
d	Any incident of loss or destruction of data or systems should be thoroughly analyzed and lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes.
e	Stock Brokers / Depository Participants should also conduct periodic drills to test the adequacy and effectiveness of the aforementioned response and recovery plan.
6	**Sharing of Information**

a	All Cyber-attacks, threats, cyber-incidents and breaches experienced by Stock Brokers / Depositories Participants shall be reported to Stock Exchanges / Depositories & 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: sbdp-cyberincidents@sebi.gov.in.
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.
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.
7	**Training and Education**
a	Stock Brokers / Depository Participants should work on building Cyber Security and basic system hygiene awareness of staff (with a focus on staff from non-technical disciplines).
b	Stock Brokers / 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.
c	The training programs should be reviewed and updated to ensure that the contents of the program remain current and relevant.
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.
8	**Systems managed by vendors**

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.
9	**SEBI and Exchange Compliances**
a	Auditor to list all applicable Circulars, Notices, Guidelines, and advisories published by SEBI and Exchanges related to Cyber Security and Cyber Resilience and mention 1- Adherence to all such Circulars, Notices, Guidelines, and advisories published 2- Reporting adherences based on prescribed periodicity in point 1 above
b	Does the Stock Broker / Depository Participant have a documented SOP for Handling and Reporting of Cyber Security Incidents Does the SOP covers all the aspects mentioned in Exchange notice no.20210430-20 dated April 30, 2021. Has the Stock Broker / Depository Participant adhered and complied to the requirements for any and all incidents in the period of audit.
c	Ref: BSE Advisory 20211102-1 on "Cyber Security Awareness Campaign" Dated 02 Nov 2021 Has the trading member / depository 1 - conducted cyber security awareness for all its employees and stakeholders 2- Shared compliance Records
d	Ref: BSE Advisory 20210430-20 on "Standard Operating Procedure (SOP) for handling cyber security incidents of intermediaries" Dated 30 Apr 2021 Does the Trading Member / Deopsitory Participant 1- Have Documented the SOP as per requirements in advisory 2- In case of happening of an incident, has -SOP adherence been evidenced -Reporting of Incident evidenced as per advisory
e	Ref: BSE Advisory 20211117-58 on “Distributed Denial of Service (DDoS) attacks on systems of intermediaries” Dated 17 Nov 2021 Are steps taken towards the adhenrence of the advisory evidenced at the Trading Member / Deopsitory Participant

f	Ref: BSE Advisory 20201127-7 on “Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions” Dated 27 Nov 2020 Are steps taken towards the adhenrence of the advisory evidenced at the Trading Member / Deopsitory Participant
10	**SECURITY OPERATION CENTER (SOC)**
10(a)	Whether organization has set-up Security Operations Center (In-house / Market SOC / Outsourced) so as to ensure that the organization is in compliance with the SEBI / Exchange guidelines regarding Cyber Security & Cyber Reslience Framework?