Cyber Security & Cyber Resilience Framework Implementation

Advisory

Kindly note that with reference to the SEBI Circular No. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03rd , 2018 on Cyber Security & Cyber Resilience framework for Stock Brokers/Depository Participants, the Exchange has formulated certain suggestive measures for broad guidance that are outlined in this presentation. These measures are indicative in nature and not exhaustive and adherence to the measures listed in this presentation alone would not result in complete conformance to SEBI Circular No. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03rd , 2018. Stock Brokers/Depository Participants are required to go through the circular in detail and ensure that all the points mentioned therein are adhered to.

SEBI Circular Summary

Sr #	Domain	Controls	Members	MIIs
2	Governance	9	9	-
3	Identification	2	2	-
4	Protection - Access Control	9	9	-
5	Protection -Physical Security	3	3	-
6	Protection- Network Security Management	4	4	-
7	Protection – Data Security	4	4	-
8	Protection - Hardening of Hardware and Software	2	2	-
9	Protection - Application Security in Customer Facing Applications	1	1	-
10	Protection - Certification of off-the-shelf products	1	1	-
11	Protection - Patch Management	2	2	-
12	Protection - Disposal of data, systems and storage devices	2	2	-
13	Protection - Vulnerability Assessment and Penetration Testing (VAPT)	4	4	-
14	Monitoring and Detection	2	2	-
15	Response and Recovery	5	5	-
16	Sharing of Information	1	1	-
17	Training and Education	3	3	-
18	Systems managed by vendors	1	1	-
19	Systems managed by MIIs	1	-	1
20	Periodic Audit	1	1	-
	TOTAL	**57**	**56**	**1**

Domain Governance

Governance – 2

Sr. #	Control Description	Suggestive Measures
2	As part of the operational risk management framework to manage risk to systems, networks and databases from cyber-attacks and threats, Stock Brokers/ Depository Participants should formulate a comprehensive Cyber Security and Cyber Resilience policy document encompassing the framework mentioned hereunder. In case of deviations from the suggested framework, reasons for such deviations, technical or otherwise, should be provided in the policy document. The policy document should be approved by the Board / Partners / Proprietor of the Stock Broker / Depository Participants. The policy document should be reviewed by the aforementioned group at least annually with the view to strengthen and improve its Cyber Security and Cyber Resilience framework	1. Define and implement a comprehensive Cyber Security and Cyber Resilience policy document. i. Define as per the regulatory guidelines prescribed by SEBI and encompassing the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) ii. The policy should capture deviations from the cyber security and cyber resilience framework iii. The policy should be reviewed and approved by the board at least annually once. **Policy Document structure** i. Scope – Covering the organizations critical systems & associated legal entities ii. Policy Governance – Should cover ❖ Ownership ❖ Review Frequency iii. Implementation – through Standard & Guidelines, Policies, Procedures, SOPs & Risk Management & Cyber Security Management Framework iv. Principles ❖ Identification ❖ Protection • Access Control • Physical Security • Network Security Management

Governance – 2 contd...

Sr. #	Control Description	Suggestive Measures
2	As part of the operational risk management framework to manage risk to systems, networks and databases from cyber-attacks and threats, Stock Brokers/ Depository Participants should formulate a comprehensive Cyber Security and Cyber Resilience policy document encompassing the framework mentioned hereunder. In case of deviations from the suggested framework, reasons for such deviations, technical or otherwise, should be provided in the policy document. The policy document should be approved by the Board / Partners / Proprietor of the Stock Broker / Depository Participants. The policy document should be reviewed by the aforementioned group at least annually with the view to strengthen and improve its Cyber Security and Cyber Resilience framework	• Data Security • Hardening Of Hardware & Software • Application Security & Vulnerability assessment & Penetration Testing (VAPT) • Certification of off-the-shelf Applications • Patch Management • Disposal of data, systems & storage devices ❖ Monitoring & Detection ❖ Response & Recovery ❖ Sharing of Information ❖ Training & Education ❖ Systems managed by Vendors ❖ Periodic Audit

Governance – 2 contd...

Sr. #	Control Description	Suggestive Measures
2	As part of the operational risk management framework to manage risk to systems, networks and databases from cyber-attacks and threats, Stock Brokers/ Depository Participants should formulate a comprehensive Cyber Security and Cyber Resilience policy document encompassing the framework mentioned hereunder. In case of deviations from the suggested framework, reasons for such deviations, technical or otherwise, should be provided in the policy document. The policy document should be approved by the Board / Partners / Proprietor of the Stock Broker / Depository Participants. The policy document should be reviewed by the aforementioned group at least annually with the view to strengthen and improve its Cyber Security and Cyber Resilience framework	2. Supporting Polices & Procedures - Adoption of best practices from International Standards such as ISO 27001, ISO 22301 or COBIT 5 i. Acceptable Usage Policy ii. Access Control Policy iii. Asset Management Policy iv. Communication Security Policy v. Cryptography Policy vi. E-Waste Policy vii. Human Resource Security viii. Information Security Compliance Policy ix. Information Security Incident Management Policy x. Information Security Policy xi. Information Systems Acquisition Development and Maintenance Policy xii. Operations Security Policy xiii. Physical and Environmental Policy xiv. Supplier Relationship Management Policy xv. Website Security Policy

Governance – 3.a

Sr. #	Control Description	Suggestive Measures
3	The Cyber Security Policy should include 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.	1. Define and implement an Information Asset Identification and Risk Assessment Methodology **2. Asset Management Policy Document structure** i. Purpose – define minimum standards to ensure ❖ Assets are documented ❖ Classified ❖ Adequately protected to prevent unauthorized/unintentional access or misuse ii. Scope – Covering the organizations critical systems & associated legal entities iii. Inventory of assets ❖ Maintain inventory of IT assets (Physical, Software, Information (digital & non digital), People & Services) ❖ Review the inventory of assets periodically to ensure its accuracy iv. Ownership of assets ❖ The owner of the asset is responsible for classifying, labelling and protecting the asset. v. Acceptable usage of asset ❖ Identify, document and implement rules for acceptable use of information and of assets associated with information and information processing facilities Return of assets

Governance – 3.a contd...

Sr. #	Control Description	Suggestive Measures
3	The Cyber Security Policy should include 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.	❖ Document and implement process to ensure Employees and external party users return all of the organizations assets in their possession upon termination of their employment, contract or agreement vi. Classification of information ❖ Classify the assets based on the impact to the business ❖ Review the classifications assigned to information at least once a year vii. Labelling of information ❖ Develop and maintain set of procedures for information labelling in accordance with the adopted information classification scheme ❖ All classified digital and non-digital information assets should be labelled. viii. Handling of asset ❖ Enforce physical and logical controls during production, storage, transit and destruction/disposal based on the classification. ❖ Asset movement should only be done for business purpose with all necessary approvals ❖ Confidential information and mails related to staff / company not to be posted on office notice boards or Internet without prior approval.

Governance – 3.a contd...

Sr. #	Control Description	Suggestive Measures
3	The Cyber Security Policy should include 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.	❖ Physical media or assets/ Non-digital Information: • Physical media must be stored in a secure environment. • Physical files containing confidential data shall be placed in drawers secured by lock and key or in a secure environment. • Hard copies / Paper documents must contain the same classification mark as the original. • Paper documents and/or media must be transferred in a sealed envelope with confidential seal and receipt confirmation must be mandatory. • All printed confidential material must be shredded prior to disposal. • CD-ROMs and other 'write-once' media must be rendered unreadable by physical destruction prior to disposal. • All reusable media used for the storage of confidential information must be securely wiped. ❖ Electronic Media / Digital Information: • Copies of the original document must contain the same classification mark as the original. • Must only be made available to internal employees or trusted third parties who have signed a non-disclosure agreement. • Adequate controls must be used to protect confidential information stored on an electronic / portable device, or where there is a requirement to store confidential information in a system.

Governance – 3.a contd...

Sr. #	Control Description	Suggestive Measures
3	The Cyber Security Policy should include 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.	• Adequate controls must be used to protect confidential information if it is transferred via external networks. (Encryption can be used if desired or Password protect the files) ix. Management of removable media ❖ Use removable media like USB Drives, Compact disks (CD and DVDs), removable disk drives, etc. only if necessary for business purpose and after due approvals from appropriate authorities ❖ Disable removable media drives on desktops ❖ Users of removable media will be responsible for any security incident due to use of removable media. (Theft of media, virus, loss of confidential data/information etc.) ❖ Information from removable media (non-company media received from external source) must not be copied to organizations assets (even if for business purposes) without checking the source for presence of any type of malicious code. ❖ Reconciliation activity of removable media should be conducted annually

Governance – 3.a contd...

Sr. #	Control Description	Suggestive Measures
3	The Cyber Security Policy should include 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.	x. Disposal of media - Reports / Printouts , Tapes / DATS / CDs / Hard Disks / Portable media ❖ Ensure secure disposal of media when no longer required, using formal procedures ❖ Ensure Secure disposal such that the data / contents of the media cannot be recovered ❖ Securely wipe /overwrite prior to disposal / re-issuance / resale or returning to vendor, hard disks of workstations and servers ❖ Magnetic media CDs and DVDs must be made unusable before being disposed. ❖ Hard disks must be made unusable by degaussing before being disposed. ❖ DAT /DLT / LTO tapes must be opened and the tape must be cut into multiple pieces prior to disposal. ❖ USB Devices/ Memory Cards of mobile phones and PDAs must be securely wiped prior to re-issuance / returning the same. Defective memory devices must be physically destroyed prior to disposal ❖ Use paper shredders to be used to securely dispose off confidential documents. ❖ Maintain records for all media that is disposed-off ❖ Perform annual review to ensure that the process of media disposal is complied. xi. Physical media transfer ❖ Physical / portable media movement to be recorded & approved by asset owner.

Governance – 3.a contd...

Sr. #	Control Description	Suggestive Measures
3	The Cyber Security Policy should include 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.	**2. Risk Assessment Methodology Framework** i. Information Asset Identification a. Department head owns overall responsibility of identification of information assets b. Assigning values to each asset in terms of Confidentiality, Integrity, and Availability (C, I, A). c. Responsible to maintain the inventory and valuation of information assets with information as follows ❖ Asset name: Name of the information asset. ❖ Asset category: Category of the information asset. • Physical - Servers, routers, switches, laptops, desktops, printers, fire extinguishers, UPS etc • Digital information - SOP, network diagram, invoices etc. • Non-digital information - hard copy of contract documents, agreements, SLAs etc • People - tester, developer, SMEs, architects, project manager, project lead etc • Service - internet service, network service, power supply, etc • Software - enterprise application software, OS, administration tools and utilities etc

Governance – 3.a contd...

Sr. #	Control Description	Suggestive Measures
3	The Cyber Security Policy should include 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.	❖ Business Process name: Business process within department using the information asset ❖ Location: Specify location of the information asset • Physical – data center, server room, cubicles, user desks, etc. • Digital information – local hard drive, storage area network, server hard drive, USB drive, SharePoint, • Non-digital information – fire proof cabinets, drawers, third party vendor (in case outsourced), lockers, • People – secured rooms, secure areas, general seating area, customer location • Service – Internet service provider, network service provider, any other third party service provider • Software – user systems, servers, etc. ❖ Description of asset: Brief description of the identified information asset ii. Information asset valuation ❖ Assess the quantitative value in terms of its importance to the business ❖ Develop a rating scale for asset value based on the impact, of a loss in its confidentiality, integrity and/or availability could have to the business ❖ The asset value is based on the traits of Confidentiality, Integrity and Availability (C, I, A) for information assets and criticality for other assets they depend on ❖ Asset Register to be reviewed and approved by the respective department Head

Governance – 3.a contd...

Sr. #	Control Description	Suggestive Measures
3	The Cyber Security Policy should include 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.	**2. Risk Assessment Methodology Framework** iii. Identification of Information asset owner, custodian and user ❖ Information asset owner: Asset owner is responsible for an information asset and is accountable for the • Determination of information sensitivity and creation of asset inventory • Ensuring that appropriate degree of protection is given • Sponsorship of regular audits for protection of information assets • Approval of access requests • Ensuring that information is updated ❖ Information asset custodian: Responsible for safeguarding the information ❖ Information asset user: Authorized to access or use the information asset iv. Identification of Business process (es) ❖ Identify core business process (es) for each of the department in scope. ❖ Capture short description of the core business departments to identify how CIA can be impacted v. Linkage of relevant information assets to the process (es) ❖ Identify critical information assets from corresponding asset register and link to the core business process. ❖ Based on the process related risks, evaluate the effectiveness of the controls implemented to safeguard the information assets

Governance – 3.a contd...

Sr. #	Control Description	Suggestive Measures
3	The Cyber Security Policy should include 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.	**2. Risk Assessment Methodology Framework** vi. Identification and evaluation of CIA concerns for process ❖ Identify confidential-integrity-availability (CIA) for each core business process vii. Identification of risks & calculation of inherent risk score ❖ Evaluate probability of the event and impact ❖ Probability of an event • likelihood of materializing the CIA concern for the business process • based upon the past incidents and have led to operational failures or delays ❖ Impact • The severity of the impact is evaluated if an event occurs ❖ Risk score = Risk Score = Probability of the event X Impact viii. Identification of existing controls & effectiveness ❖ Evaluate effectiveness of the existing controls implementation ix. Calculation of current risk score ❖ Calculate current risk score after considering the probability of the occurrence of the event, impact and existing controls that are implemented effectively. ❖ Resultant risk score determines the severity of the risk. ❖ The higher the risk score higher is the risk

Governance – 3.a contd...

Sr. #	Control Description	Suggestive Measures
3	The Cyber Security Policy should include 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.	**2. Risk Assessment Methodology Framework** viii. Risk treatment ❖ Risk treatment (mitigation) involves prioritizing, evaluating, and implementing appropriate controls selected during the treatment • Risk avoidance: Deciding by not going ahead with an activity likely to generate risk • Risk treatment (mitigation): ✓ Reduce the probability – By reducing probability of the occurrence of the event ✓ Risk transfer: By arranging another party to compensate for the loss, such as purchasing insurance ✓ Risk acceptance: The organization accepts the risk ❖ Risk Acceptance Criteria: As an exception, certain high and/or medium risk may be accepted with an appropriate business justification ❖ Risk owner shall accept the risk and provide the business justification. ❖ The accepted risk shall be reviewed periodically. ix. Calculation of residual risk score ❖ Residual risk is the remaining risk after management has taken action to alter the risk's likelihood or impact

Governance – 3.a contd...

Sr. #	Control Description	Suggestive Measures
3	The Cyber Security Policy should include 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.	**2. Risk Assessment Methodology Framework** viii. Identification of risk owner ❖ The person must have the authority to manage the risk ❖ The person will have the accountability towards the risk ix. Review of Risk Assessment - Risk assessment, the level of residual risks, and identified acceptable risks are reviewed at least on an annual basis

Governance – 3.b

Sr. #	Control Description	Suggestive Measures
3	The Cyber Security Policy should include the following process to identify, assess, and manage Cyber Security risk associated with processes, information, networks and systems: b. 'Protect' assets by deploying suitable controls, tools and measures.	1. Define and implement a process to protect assets by deployment of suitable controls, tools and measures **2. Information security policy structure** i. Purpose – Principles to guide, provide direction to, and drive decision making to ensure appropriate protection of the organization's information assets ii. Scope – Covering the organizations assets & associated legal entities iii. Information Security Objective ❖ Confidentiality - available on need to know basis ❖ Integrity - to ensure completeness and accuracy ❖ Availability - to ensure the timely recovery of all information and access by authorized individuals ❖ User Authorization - uniquely identifiable user with access permissions based on their business needs ❖ Accountability - responsible for the appropriate use, protection and privacy of these assets ❖ Continuity - to maintain continuity of operations from business and technology perspectives ❖ Trust - Partners, vendors and service providers to meet or exceed organizations security requirements

Governance – 3.b contd...

Sr. #	Control Description	Suggestive Measures
3	The Cyber Security Policy should include the following process to identify, assess, and manage Cyber Security risk associated with processes, information, networks and systems: b. 'Protect' assets by deploying suitable controls, tools and measures.	**2. Information security policy structure** iv. ISMS Exceptions – To address deviations to the Policy due to business needs, technical challenges etc. v. Policy Governance ❖ Ownership ❖ Review Frequency vi. IS Governance ❖ Governing Committee & IS Organization ❖ Supporting Documentation • Information Security Policies • Information security Procedures vii. Compliance - Management to ensure compliance and take corrective actions when security controls are not in accordance with the policies viii. Disciplinary Action – for individual violating the provisions in the information security policies

Governance – 3.b contd...

Sr. #	Control Description	Suggestive Measures
3	The Cyber Security Policy should include the following process to identify, assess, and manage Cyber Security risk associated with processes, information, networks and systems: b. 'Protect' assets by deploying suitable controls, tools and measures.	**3. Security measures** i. Security tools & documented process/Manual for each of the security devices ❖ Data leakage prevention, ❖ Digital Rights Management ❖ Database Active Monitoring, ❖ Privileged Identity access management, ❖ Security information and event management, ❖ IDS ❖ IPS, ❖ Network Anomaly Detection ❖ Ant phishing and Antimalware ❖ Data Encryption (at Rest & In Motion) ❖ Adequate access control (Logical and Physical). ❖ Adequate vulnerability identification, application testing, Network security, hardening and patch management of critical systems and secure disposal of sensitive information.

Governance – 3.c,d

Sr. #	Control Description	Suggestive Measures
3	The Cyber Security Policy should include the following process to identify, assess, and manage Cyber Security risk associated with processes, information, networks and systems: 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.	1. Define and implement Incident Management process to monitor and detect incidents, anomalies and attacks **2. Incident management policy structure** i. Purpose – ❖ To identify and resolve information security incidents quickly and effectively, ❖ Minimize business impact and reduce the risk of similar incidents occurring ii. Scope – Covering the organizations assets & associated legal entities iii. Management of Information Security Incidents ❖ Responsibilities and Procedures • Conduct training to make personnel aware of process for reporting any information security events and weaknesses • Document roles and responsibilities for managing Information security incidents ❖ Reporting information security events & security weaknesses • Incidents to be reported such as ✓ Ineffective security control ✓ Breach of information integrity, confidentiality or availability expectations ✓ Human errors; ✓ Non-compliances with policies or guidelines; ✓ Breaches of physical security arrangements;

Governance – 3.c,d contd...

Sr. #	Control Description	Suggestive Measures
3	The Cyber Security Policy should include the following process to identify, assess, and manage Cyber Security risk associated with processes, information, networks and systems: 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.	**2. Incident management policy structure** ✓ Uncontrolled system changes; ✓ Mal functions of software or hardware; ✓ Access violations • Report information security events through appropriate channels – portals, emails, telephone or personal communication • Install monitoring components for critical servers for capturing security events • Review the system generated alerts/events and fine-tune ❖ Assessment of and decision on information security events • Detect, categorize and investigate in a defined manner • Classification of incidents basis of business impact • Assign priority level ❖ Response to information security incidents • Assign incident to provide resolution. • Analyze to identify root cause and to take corrective action to prevent reoccurrence based on severity. • Refer SOP / run books to handle different types. • Communicate the incident status to affected parties and/or appropriate stakeholder(s) • Resolve within predefined time and document the details of resolution

Governance – 3.c,d contd...

Sr. #	Control Description	Suggestive Measures
3	The Cyber Security Policy should include the following process to identify, assess, and manage Cyber Security risk associated with processes, information, networks and systems: 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.	• Escalate as per Escalation Matrix, if not resolved on time. • Review incidents on periodic basis . ❖ Learning from information security incidents • Monitor and review for critical security breaches as and when required. • Record learnings from critical security breaches • Update end users through training, updates to policies, procedures etc. ❖ Collection of evidence • Identify, collect and securely store necessary information / data which can serve as evidence. • Collect evidence in compliance to legal requirements as applicable. ❖ Assessment of and decision on information security events • Detect, categorize and investigate in a defined manner • Classification of incidents basis of business impact • Assign priority level

Governance – 3.e

Sr. #	Control Description	Suggestive Measures
3	The Cyber Security Policy should include the following process to identify, assess, and manage Cyber Security risk associated with processes, information, networks and systems: e. 'Recover' from incident through incident management and other appropriate recovery mechanisms	1. Define a Disaster recovery and business continuity framework • Business continuity policy • Business continuity plan **2. BCP Policy Structure** i. Purpose – ❖ Guidelines for developing, maintaining and exercising Business Continuity Plan (BCP) ❖ Ensure emergency response, resumption and recovery of operations and business activities in the event of disaster ii. Scope - Covering the organizations assets & associated legal entities iii. Information security continuity ❖ Planning Information Security Continuity • Disaster Escalation Hierarchy • Business Continuity Structure ❖ Implementing Information Security Continuity • Primary Data Center Set Up • Near Site Setup ❖ Evaluate Information Security Continuity • NS/BCP/DR Drills and Testing • BCP Training and Awareness • BCP DR Annual Audit

Governance – 3.e contd....

Sr. #	Control Description	Suggestive Measures
3	The Cyber Security Policy should include the following process to identify, assess, and manage Cyber Security risk associated with processes, information, networks and systems: e. 'Recover' from incident through incident management and other appropriate recovery mechanisms	**2. BCP Policy Structure** • BCP DR Annual Audit • Non conformities and corrective action • Continual Improvement ❖ Periodic Policy Review i. Redundancies ❖ Availability of information processing facilities • BCP/DR Setup ii. Roles & Responsibilities

Governance

Sr. #	Control Description	Suggestive Measures
4	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.	1. The Cyber Security & Cyber Resilience Policy should encompasses the principles defined for NCIIPC. ❖ Implement NCIIPC Principles ❖ Define and implement process of tracking the compliance of NCIIPC principles ❖ Conduct periodic review of NCIIPC controls • 40 Control Areas - 400 sub controls

Governance

Sr. #	Control Description	Suggestive Measures
5	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.	1. Is the organization certified or has incorporated best practices such as ISO 27001, ISO 22301 or COBIT 5 i. Information Policies and procedures governance framework basis of the standards ❖ Acceptable Usage Policy ❖ Access Control Policy ❖ Asset Management Policy ❖ Communication Security Policy ❖ Cryptography Policy ❖ E-Waste Policy ❖ Human Resource Security ❖ Information Security Compliance Policy ❖ Information Security Incident Management Policy ❖ Information Security Policy ❖ Information Systems Acquisition Development and Maintenance Policy ❖ Operations Security Policy ❖ Physical and Environmental Policy ❖ Supplier Relationship Management Policy ❖ Website Security Policy

Governance

Sr. #	Control Description	Suggestive Measures
6	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	1. The organization should appoint/designate a Senior Official – "Designated Officer" 2. The "Designated Officer" should be a part of Governing Committee and Internal Technology Committee 3. The Cyber Security & Cyber Resilience Policy should outline his roles and responsibilities 4. The roles & responsibilities of the Designated Officer to include i. Assessment ii. Identification iii. Reduction of cyber security risks, iv. Response to incidents, v. Establish appropriate standards and controls, vi. Direct the establishment and implementation of processes and procedures as per the cyber security and resilience policy approved by the Board

Governance

Sr. #	Control Description	Suggestive Measures
7	The Board / Partners / Proprietor of the Stock Brokers / Depository Participants shall constitute 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.	1. Oversight Technology Committee and IT Strategy Committee to review the implementation of the Cyber Security & Cyber Resilience Policy on **a half yearly basis** encompassing : i. Current IT, Cyber Security & Cyber Resilience Capabilities ii. Goals & Target to be achieved to improve the security posture iii. Plans to further strengthen 2. Half Yearly Review Reports 3. Minutes of the Meetings 4. Compliance dashboard 5. Metrics for each of the control defined, implemented and tracked 6. The reports to be placed in front of Board / Partners / Proprietor

Governance

Sr. #	Control Description	Suggestive Measures
8	Stock Brokers / Depository Participants should establish a reporting procedure to facilitate communication of unusual activities and events to the Designated Officer in a timely manner	1. Define a reporting procedure to communicate the unusual activities and events to the "Designated Officer" ❖ Communication procedure ❖ Escalation matrix ❖ .Roles and responsibilities of CMT
9	The Designated officer and the technology committee of the Stock Brokers / Depository Participants should periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen Cyber Security and cyber resilience framework	1. The Technology Committee and the Designated Officer should review instances of cyber attacks that have occurred domestically and globally 2. List steps to be taken post management's review of cyber attacks that have occurred domestically and globally ❖ Communication procedure ❖ Periodic alerts received from governing bodies such as CERT-in, ISACA, etc and communicating the same to the Designated Officer
10	Stock Brokers / Depository Participants should define 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 Stock Brokers / Depository Participants towards ensuring the goal of Cyber Security	1. Define Roles and responsibilities related to cyber security of all the vendors, outsourced staff, employees who access or use organizations systems and network ❖ Cyber Security & Cyber Resilience Policy ❖ Access control Policy and Procedure ❖ Acceptable Usage Policy • Define roles and responsibilities of all vendors, outsources staff, employees who has access to NSE systems and network.

Domain Identification

Identification

Sr. #	Control Description	Suggestive Measures
11	Stock Brokers / Depository Participants should identify critical assets based on their sensitivity and criticality for business operations, services and data management. 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.	1. Identify critical assets based on sensitivity and criticality of business operations, services and data management ❖ Asset identification and classification procedure ❖ List of critical assets 2. Maintain & Review an inventory of assets (i.e. hardware and systems, software and information assets (internal and external) on a periodic basis ❖ Asset inventory list/ asset management tool 3. Maintain & Review network resources, network connections and data flows on a periodic basis ❖ Network Architecture/ diagram
12	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	1. Maintain , Review & Update Cyber Risks (threats & vulnerabilities) on a periodic basis ❖ Threat and vulnerability database 2. Define a Cyber risk management process taking into account the likelihood of such threats and impact on the business ❖ Risk management procedure 3. Implement security controls post the cyber risk assessment process to commensurate the criticality ❖ Risk register ❖ Risk treatment plan ❖ Risk acceptance

NSE

1994 25 2019

Domain Protection – Access Control

Protection – Access Control

Sr. #	Control Description	Suggestive Measures
13	No person by virtue of rank or position should have any intrinsic right to access confidential data, applications, system resources or facilities.	1. Define Access Control Policy and Procedure 2. Define Physical Access Control Policy and Procedure 3. Provision accesses on need to know/role basis and on the principle of least privilege
14	Any access 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	1. Define the access provisioning & de-provisioning process for systems, applications, databases, networks and network services encompassing ❖ Purpose of access ❖ Approval for access requested ❖ Period of accesses required - temporary or permanent 2. Define a process to perform access rights review on a periodic basis 3. Define and implement stringent authentication mechanism for OS, Database, System and Network devices

Protection – Access Control

Sr. #	Control Description	Suggestive Measures
15	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	1. Define and implement a Password policy - for AD authenticated and non AD authenticated application, Network devices, User system, default password, admin users with parameters such as ❖ Complexity - 12 characters with upper case and lower case letters, numerals and special characters ❖ Password change - 30-90 days ❖ Password of privileged account - 25 days ❖ Password age - 1 day ❖ Password history - 5 ❖ Wrong attempts -5 ❖ Privilege account wrong attempts - 3 2. Implement AD authentication for all systems 3. For network devices authentication integrate with TACACS, AD. ❖ Minimum PIN Length - 4 characters ❖ Maximum PIN Length - 8 characters ❖ Maximum token age - 60 seconds ❖ Maximum passcode age -60 seconds 4. Define and implement a formal secure log-on procedure to access to systems and applications ❖ User registration process and procedure for secure log on ❖ Each user should be assigned with user id and credentials

Protection – Access Control

Sr. #	Control Description	Suggestive Measures
15	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	1. Define and implement a process for Password creation and communication ❖ Document the process for passwords communicated to personnel via secure medium ❖ Distribution of initial passwords are controlled such that the user id and password are either encrypted or communicated separately/ secretly ❖ Privileged passwords, emergency account passwords are communicated through tamper proof envelope. ❖ Document procedure for managing secret authentication information of users 2. Personnel should be forced to change the default password at first log in 3. Disable Reversible encryption 4. Password are to be masked on the screen while being entered

Protection – Access Control

Sr. #	Control Description	Suggestive Measures
16	All critical systems of the Stock Broker/ Depository Participant accessible over the internet should have two-factor security (such as VPNs, Firewall controls etc.)	1. Multifactor authentication mechanism implemented for all the application which can be accessed through internet ❖ OTP (Email or SMS) ❖ Password ❖ Biometric ❖ VPN
17	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.	1. Define and implement a Log management and monitoring policy and procedure for all systems ❖ Log system operator, system administrator and privileged access user activities ❖ Implement a central log (sys log) server 2. Ensure appropriate security of Logs against unauthorized access by maintaining ❖ an access list as to who has access to the logs, ❖ change or delete permissions that have been granted ❖ retention periods for the logs 3. Records of user logs, audit logs are to be maintained for at least 2 years 4. Records of user logs, audit logs are to be maintained and stored in an encrypted form 5. Define and implement a process to review all logs (System, Server, Firewall, Network) periodically, along with details of responsibility for the review, as well as any other information relevant to reviewing logs. 6. Document details of procedures for retrieving of logs for investigative purposes

Protection – Access Control

Sr. #	Control Description	Suggestive Measures
18	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	1. Document and implement a procedure for management of privileged access rights with stringent password policy parameters ❖ Password expiry – 30 days ❖ Password history – 6 ❖ Wrong attempts – 2 2. Maintain a list of privilege users 3. Document and implement a procedure for periodic review of privileged ids access rights (quarterly) 4. Disallow privileged users from accessing systems logs, however if they do have accesses , record and capture privilege users access logs for all activities 5. Disallow remote access to users with privilege access to systems. However if accesses are required define and implement a process for accessing system remotely through any secure medium (VPN)

Protection – Access Control

Sr. #	Control Description	Suggestive Measures
19	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.	1. Define and implement procedures to access critical system, network and other computer resources user access provisioning and information access restriction for employees 2. Define and implement procedures to access critical system, network and other computer resources user access provisioning and information access restriction for vendors and outsourced staff ❖ Third party vendor relationship management ❖ Third party on boarding and off boarding process 3. Monitor accesses to critical system, network and other computer resources 4. Restrict access to critical system, network and other computer resources
20	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.	1. Define and implement internet access policy for internet and internet based services such as social media sites, cloud-based internet storage sites, etc. 2. Implement a mechanism to monitor internet activity

Protection – Access Control

Sr. #	Control Description	Suggestive Measures
21	User Management must address deactivation of access of privileges of users who are leaving the organization or whose access privileges have been withdrawn.	1. Document and implement a procedure for removal and adjustment of access rights along with review of user access rights.

Domain Protection – Physical Security

Protection – Physical Security

Sr. #	Control Description	Suggestive Measures
22	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	1. Define and implement measures for security perimeters to protect areas that contain either sensitive or critical information and information processing facilities 2. Document and maintain list of secure areas within the organization 3. Define and implement processes for Visitor Management ❖ Ensure visitors are required to sign-in, receive ID badge and are escorted while on premises
23	Physical access to the critical systems should be revoked immediately if the same is no longer required	1. Define and implement process for removal of physical access to critical system. ❖ Physical access to critical system to be revoked immediately if the same is not required 2. Define and implement process for periodic review of physical access to critical systems (Monthly)
24	Stock Brokers / Depository Participants should ensure that the perimeter of the critical equipment 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	1. Implement controls to restrict access to the server/computer room • e.g., written authorizations, type of access control system, biometrics, mantrap, re-certification of access, maintenance of access, visitor access, service technician access, business versus non-business hours 1. Place security guards at the perimeter/entrance and exit of the critical equipment's room 2. Install CCTV cameras at the perimeter/entrance and exit of the critical equipment's room 3. Install access control mechanism such as biometrics/mantraps/bollards etc. to access the critical equipment's room

Domain Protection – Network Security

Protection – Network Security Management

Sr. #	Control Description	Suggestive Measures
25	Stock Brokers / Depository Participants should establish baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within their IT environment. The LAN and wireless networks should be secured within the Stock Brokers / Depository Participants' premises with proper access controls.	1. Define and implement baseline standard for configuration management to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices 2. Define a process to conduct configuration review to verify that the baseline configuration policy implemented is consistent ❖ Define frequency for hardening checklist configuration review. ❖ Maintain tracking of closure of findings / observations reported. 3. Define access control policy for secure LAN and wireless networks
26	For algorithmic trading facilities, adequate measures should be taken to isolate and secure the perimeter and connectivity to the servers running algorithmic trading applications	

Protection – Network Security Management

Sr. #	Control Description	Suggestive Measures
27	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	1. Install internal and external firewalls. Segregate network logically such as ❖ Internal network ❖ External network ❖ Internet network ❖ Management network. 2. Servers which require internet access and accessed from internet should be placed in DMZ segment. 3. Servers such as mail gateway, DNS server etc. should be placed in DMZ segment. 4. Deploy IDS to monitor malicious and suspicious traffic. 5. Configure IPS at perimeter to detect and block malicious traffic . Signatures with high priority should be blocked immediately . Medium and low priority signatures should be configured to generate events 6. Monitor and manage all security incidents 7. Integrate security devices with an SIEM for analyzing and monitoring security incidents. 8. Maintain an updated network architecture diagram detailing placement of firewall, IDS and IPS 9. Conduct periodic review of the network architecture. 10.Install security devices for monitoring such as ❖ Security incident and event management (SIEM) ❖ Privileged identity management (PIM) ❖ Data leakage prevention (DLP)

Protection – Network Security Management

Sr. #	Control Description	Suggestive Measures
27	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	❖ Database activity monitoring (DAM) ❖ Documents rights management (DRM) ❖ Network anomaly detection system (NADS) ❖ Anti-Malware services for website ❖ Anti-Phishing services for website ❖ Threat tracking services ❖ DDoS protection service
28	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.	1. Install antivirus and antimalware solutions on computer system for endpoint devices and servers ❖ HIPS ❖ NIPS ❖ Antivirus ❖ Antimalware 2. Implement a central server to scan and deploy latest signature updates periodically 3. Define and implement a process for periodic scanning for all information systems ❖ Maintain dashboard report (Weekly, monthly) and compliance tracker.

Domain Protection – Data Security

Protection – Data Security

Sr. #	Control Description	Suggestive Measures
29	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	1. Define and implement an effective data classification policy 2. Deploy different technologies for encryption of traffic at : ❖ Local networks ❖ WAN networks ❖ Desktops and Laptops ❖ Internet links ❖ Applications 3. Define Cryptographic policy and procedure to protect critical information at rest with various layers of security ❖ disk encryption ❖ database encryption
30	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.	1. Data protection policy to restrict transfer of information in clear text and if so are there processes to detect violations 2. Define process to share data with external third parties 3. List various security mechanism used to share the data with third parties

Protection – Data Security

Sr. #	Control Description	Suggestive Measures
31	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	1. Data protection policy to restrict the information that can be stored on portable devices such as phones 2. Define and implement a Mobile Device Policy 3. Identify and implement technologies used for mobility security
32	Stock Brokers / Depository Participants should allow only authorized data storage devices within their IT infrastructure through appropriate validation processes.	1. Define and implement process of commission of laptops or any authorized devices to employees 2. Define and implement Hardening policy for laptop/desktop

Domain Protection – Hardening of Hardware & Software

Protection – Hardening of Hardware & Software

Sr. #	Control Description	Suggestive Measures
33	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	1. Define and implement approved hardening guidelines for ❖ OS (Windows , LINUX etc.) ❖ Desktops ❖ Network Devices (Firewall, Router, Switch etc) ❖ Middleware's (Weblogic, Apache, IIS etc.) ❖ Databases (Oracle, SQL etc.) 2. Review the hardening documents on a periodic basis. 3. Ensure that system default passwords are changed i. Default system password such as root/SYS/System etc. should be changed immediately after installation/implementation of information system. ii. Default system accounts such as administrator/guest etc shall be renamed/disabled/deleted as applicable 4. Unnecessary services such as administrative rights, USB access should be removed or disabled in equipment's/software 5. Define and implement a System Induction process . Hardening procedures should be defined as a part of system/device commissioning and decommissioning

Protection – Hardening of Hardware & Software

Sr. #	Control Description	Suggestive Measures
34	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	1. Block or disable open ports which are not in use or can potentially be used for exploitation 2. Define and implement a process for opening of ports/services 3. Conduct periodic port scanning conducted for all the open ports? 4. Monitor all the open ports and take appropriate measures to secure them

Domain Protection – Application Security in Customer Facing Applications

Protection – Application Security in Customer Facing Applications

Sr. #	Control Description	Suggestive Measures
35	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 paramount as they carry significant attack surfaces by virtue of being available publicly over the Internet for mass use. An illustrative list of measures for ensuring security in such applications is provided in Annexure C	1. Applications over the Internet should be password protected with a multifactor mechanism, at the minimum a 2FA should be implemented. ❖ OTP – SMS & Email ❖ Physical Token – PIN & Password ❖ Software Token ❖ VPN ❖ Biometric devices ❖ PKI 2. Reasonable minimum length and complexity of passwords should be enforced. ❖ Password parameters • Complexity - 12 characters with upper case and lower case letters, numerals and special characters • Password change - 30-90 days • Password of privileged account - 25 days • Password age - 1 day • Password history - 5 • Wrong attempts -5 • Privilege account wrong attempts - 3

Protection – Application Security in Customer Facing Applications

Sr. #	Control Description	Suggestive Measures
35	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 paramount as they carry significant attack surfaces by virtue of being available publicly over the Internet for mass use. An illustrative list of measures for ensuring security in such applications is provided in Annexure C	❖ PIN parameters • Minimum PIN Length - 4 characters • Maximum PIN Length - 8 characters • Maximum token age - 60 seconds • Maximum passcode age -60 seconds 3. Passwords, security PINs etc. should never be stored in plain text and should be one-way hashed using strong cryptographic hash functions (e.g.: bcrypt, PBKDF2) before being committed to storage to ensure that stored password hashes are never transformed into the original plaintext values under any circumstances. 4. For applications installed on mobile devices , a cryptographically secure biometric two-factor authentication mechanism may be used. 5. After a reasonable number of failed login attempts into Applications, the Customer's account can be set to a "locked" state where further logins are not possible until a password and authentication reset is performed via an out-of-band channel validation, for instance, a cryptographically secure unique link that is sent to the Customer's registered e-mail, a random OTP (One Time Password) that is sent as an SMS to the Customer's registered mobile number, or manually by the Broker after verification of the Customer's identity etc.

Protection – Application Security in Customer Facing Applications.....Contd

Sr. #	Control Description	Suggestive Measures
35	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 paramount as they carry significant attack surfaces by virtue of being available publicly over the Internet for mass use. An illustrative list of measures for ensuring security in such applications is provided in Annexure C	6. Avoid forcing Customers to change passwords at frequent intervals which may result in successive, similar, and enumerated passwords. 7. Educate Customers to choose strong passphrases. Customers may be reminded within reasonable intervals to update their password and multi-factor credentials, and to ensure that their out-of-band authentication reset information (such as e-mail and phone number) are up-to-date. 8. Both successful and failed login attempts against a Customer's account may be logged for a reasonable period of time. After successive login failures, it is recommended that measures such as CAPTCHAs or rate-limiting be used in Applications to thwart manual and automated brute force and enumeration attacks against logins

Domain Protection – Certification of off-the-shelf products

Protection – Certification of off-the-shelf products

Sr. #	Control Description	Suggestive Measures
36	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) Standardization Testing and Quality Certification (Ministry of Electronics and Information Technology). Custom developed / in-house software and components need not obtain the certification, but have to undergo intensive regression testing, configuration testing etc. The scope of tests should include business logic and security controls	1. Off the shelf products used for core business should bear Indian Common criteria certification of Evaluation Assurance Level 4 provided by (STQC) Standardization Testing and Quality Certification (Ministry of Electronics and Information Technology). 2. Define and implement secure coding guidelines and best practices to be used during application development 3. The tests should cover business logic, security controls testing , system performance testing and stress-load testing 4. Conduct regression testing before new or modified system is implemented ❖ Parallel Runs ❖ Load Testing ❖ Unit Testing ❖ Integration Testing 5. Conduct application security testing carried out for all the critical application ❖ Grey Box ❖ White Box ❖ Code Reviews

NSE

1994 25 2019

Domain Protection – Patch Management

Protection – Patch Management

Sr. #	Control Description	Suggestive Measures
37	Stock Brokers / 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.	1. Define and implement approved patch management policy and procedure ❖ Frequency ❖ Patch deployment process 2. Scope should encompass OS, Database, Middleware, Network devices, Security software, storage devices 3. Define parameters for classifying patches in ❖ Very High (VH) ❖ High (H), ❖ Medium (M) ❖ Low (L) 4. Define parameters or criteria for prioritizing the patches to be installed 5. Maintain details of patches installed such as testing results, approvals, rollback plan, risk approvals, implementation timeframe 6. All security patches and operational patches should be fixed within 60 days of identification 7. Patches identified as critical/emergency should be fixed immediately

Protection – Patch Management

Sr. #	Control Description	Suggestive Measures
38	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	1. Test all critical patches in a test environment before deploying on production environment. 2. Maintain details of patches installed such as testing results, approvals, rollback plan, risk approvals, implementation timeframe, test environment

Domain Protection – Disposal of Data, Systems & Storage Devices

Protection – Disposal of Data, Systems & Storage Devices

Sr. #	Control Description	Suggestive Measures
39	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	1. Define and implement asset management policy and procedure for all types of information, devices and equipment's 2. Format and degauss all media and systems to ensure data is not recoverable prior to disposal or decommissioning 3. Maintain checklist for media formatting or disposal 4. Maintain evidence of media disposal for last 3 months at a minimum.

Protection – Disposal of Data, Systems & Storage Devices

Sr. #	Control Description	Suggestive Measures
40	Stock Brokers / Depository Participants should formulate a data-disposal and data-retention policy to identify the value and lifetime of various parcels of data	1. Define and implement a data-disposal and data-retention policy

Domain Protection – Vulnerability Assessment & Penetration Testing

Protection – Vulnerability Assessment & Penetration Testing (VAPT)

Sr. #	Control Description	Suggestive Measures
41	Stock Brokers / Depository Participants should regularly conduct vulnerability assessment to detect security vulnerabilities in their IT environments exposed to the internet	1. Define and implement a Vulnerability assessment and penetration testing procedure and calendar 2. Conduct periodic tests for all the critical application, server, network devices, data bases etc . ❖ Quarterly • Vulnerability Assessment (Patch Compliance) • External Penetration Tests ❖ Annual • Configuration Assessment (Hardening) 3. Define parameters to classify vulnerabilities into High, Medium and Low 4. Participate in Cyber Security Drills 5. Perform vulnerability scanning, penetration testing and configuration reviews (hardening) prior to the commissioning of internet facing/exposed system and applications
42	Stock Brokers / Depository Participants with systems publicly available over the internet should also carry out penetration tests, at-least once a year, in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks that are exposed to the internet In addition, Stock Brokers / Depository Participants should perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system that is accessible over the internet.	

Protection – Vulnerability Assessment & Penetration Testing (VAPT)

Sr. #	Control Description	Suggestive Measures
43	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	1. Define and implement a process to communicate vulnerabilities to vendors 2. Incorporate clauses in agreement for vendors to close observations & vulnerabilities 3. Track to closure
44	Remedial actions should be immediately taken to address gaps that are identified during vulnerability assessment and penetration testing	1. Describe the corrective action procedure for all the vulnerabilities identified in the VAPT exercise carried out 2. Maintain tracker for closure and corrective action of VAPT 3. Define the timelines for closures of identified vulnerabilities basis of the severity

NSE

1994 25 2019

Domain Monitoring & Detection

Monitoring & Detection

Sr. #	Control Description	Suggestive Measures
45	Stock Brokers / Depository Participants should establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events / alerts and timely detection of unauthorized or malicious activities, unauthorized changes, unauthorized access and unauthorized 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	1. Define and implement procedure for security incident monitoring, identification, classification and response. ❖ Incident management procedure 2. Monitor security logs of systems, applications and network devices for potential anomalies.
46	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,	1. Define and implement procedure to monitor capacity utilization of critical system and networks ❖ Define threshold alerts for critical system and alerts ❖ Implement thresholds configured in monitoring tools

Domain Response & Recovery

Response & Recovery

Sr. #	Control Description	Suggestive Measures
47	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	1. Define and implement a process for Incident response and analysis – inclusive of ❖ Root cause analysis ❖ Forensic analysis ❖ Corrective action ❖ Mitigation procedure ❖ Eradication ❖ Escalation matrix ❖ Incident communication
48	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	1. Define and implement a Business continuity Policy and Plan 2. Conduct Business impact analysis for all processes 3. Ensure RPO and RTO for all the critical business processes are in line with the RTO and RPO requirement specified by SEBI

Response & Recovery

Sr. #	Control Description	Suggestive Measures
49	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.	1. Maintain an updated Incident response management/crisis management team 2. Define the roles, responsibilities and actions to be performed by the employees and contractors/vendor in the event of cyber attacks in the incident response plan
50	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	1. Conduct root cause analysis for all the security incidents 2. Maintain details of all the security incidents including corrective action taken in knowledge database which can be used to strengthen security mechanism and improve recovery planning and process
51	Stock Brokers / Depository Participants should also conduct suitable periodic drills to test the adequacy and effectiveness of the aforementioned response and recovery plan	1. Conduct periodic drills to test the adequacy and effectiveness of the response and recovery plan ❖ Fire Drill ❖ Cyber Security Drill ❖ IT DR 2. Incorporate learnings from periodic drills during the review/update of the response and recovery plan

Domain
Sharing of Information

Sharing of Information

Sr. #	Control Description	Suggestive Measures
52	Quarterly reports containing information on cyber-attacks and threats 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 should be submitted to Stock Exchanges / Depositories	1. Maintain a central repository/database to capture information on cyber attacks and threats experienced by the organization. 2. Submit quarterly reports on cyber security attacks/threats and the corresponding mitigation measure taken by your organization to SEBI.

Domain
Training & Education

Training & Education

Sr. #	Control Description	Suggestive Measures
53	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).	1. Define and implement a training and awareness programme ❖ Newsletters ❖ Screen Savers ❖ Wallpapers ❖ Videos ❖ Posters ❖ Induction Sessions ❖ Annual Awareness Refresher ❖ Simulations ❖ Drills
54	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.	1. Conduct training on information security for employees during induction 2. Conduct periodic refresher training on information security for employees, vendor/contractors 3. Conduct periodic focused information security training related to the line of business to increase awareness levels and skillset of staff from non technical disciplines

Training & Education

Sr. #	Control Description	Suggestive Measures
55	The training programs should be reviewed and updated to ensure that the contents of the program remain current and relevant	1. Define the training programme ❖ Training calendar 2. Review and update the training program 3. Review and update the training content periodically considering the changing cyber risk landscape ❖ Maintain version history and versions of the training content

Domain
Systems managed by Vendors

Systems managed by Vendors

Sr. #	Control Description	Suggestive Measures
56	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	1. Enforce or direct vendors or services providers to implement information security framework 2. Define a third party/ vendor risk process to ensure vendors have implemented similar standards of information security ❖ Vendor agreements ❖ Third party audit/assessment reports • Backup and Restoration Controls • Change Management Procedures. • Compliance • Human Resource Security • Incident Management and Response. • Information Security Incident Management • Information Transfer • Logical Access policy and controls. • Operational Infrastructure. • Operations Security • Patch Management • Physical and Environmental Security • Service Level Adherence. • Software Change Management Procedures/ SDLC. • Software Testing Procedures and Test records.

Systems managed by Vendors

Sr. #	Control Description	Suggestive Measures
56	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	• Supplier Relationships • System Acquisition, Development and Maintenance • System and Application Access Control • Technical Vulnerability Management • Third Party Controls • User Awareness

Domain Systems managed by MIIs

Systems managed by MIIs

Sr. #	Control Description	Suggestive Measures
57	Where applications are offered to customers over the internet by MIIs (Market Infrastructure Institutions), for eg.: NSE's NOW, BSE's BEST etc., the responsibility of ensuring Cyber Resilience on those applications reside with the MIIs and not with the Stock Broker/ Depository Participant. The Stock Broker/ Depository Participants exempted from applying the aforementioned guidelines to such systems offered by MIIs such as NOW, BEST, etc	1. Not Applicable

Domain Periodic Audit

Periodic Audit

Sr. #	Control Description	Suggestive Measures
58	The Terms of Reference for the System Audit of Stock Brokers specified vide circular no. CIR/MRD/DMS/34/2013 dated November 06, 2013,shall accordingly stand modified to include audit of implementation of the aforementioned areas. The Depository Participants and Type I Stock Brokers (as defined in CIR/MRD/DMS/34/2013 dated November 06, 2013) shall arrange to have their systems audited on an annual basis by a CERT-IN empanelled auditor or an independent CISA/CISM qualified auditor to check compliance with the above areas and shall submit the report to Stock Exchanges / Depositories along with the comments of the Board/ Partners / Proprietor of Stock Broker/ Depository Participant within three months of the end of the financial year.	1. The circular shall be effective from April 1, 2019 2. Incorporate the circular as scope in the existing scope 3. Conduct the audit as per SEBI System audit framework 4. Ensure that the auditor is selected as per auditor selection norm mentioned in the System audit framework 5. CERT-IN empanelled auditor or an independent CISA/CISM qualified auditor to conduct audit 6. Submit the report to Stock Exchanges / Depositories along with the comments of the Board / Partners / Proprietor of Stock Broker/ Depository Participant within three months of the end of the financial year.

Thank You