Motilal Oswal Financial Service Limited

Cyber Security & Cyber Resilience Policy

Document identifier - MOFSL/POL/010/CyberResilience

Version number - 1.8

Effective date – 25th April 2025

Document Details

Sr No.	Type of Information	Document Data
1	Document Title	Cybersecurity and Cyber Resilience Policy
2.	Document Version	1.8
3.	Date of Release	25th April 2025
4.	First Published Date	11th May 2019
5	Classification	Confidential
6.	Document Owner	Mr. Pankaj Purohit
7.	Document Author	IT Security Team
8.	Distribution	All Employees & relevant third-party
9	Periodicity of Policy and procedure Review	Bi-Annually

Document Change Control

Version	Date	Reviewed By	Approved By	Release Date	Nature of Change
1.0	11th May 2019	Mr. Amit Ghodekar and Mr. Pankaj Purohit	Board of Directors	11th May 2019	First Release
1.1	11th May 2020	Mr. Pankaj Purohit	Board of Directors	11th May 2020	Annually Reviewed
1.2	21st Dec 2021	Mr. Pankaj Purohit	Board of Directors	21st Dec 2021	Annually Reviewed
1.3	20th Sep 2022	Mr. Pankaj Purohit	Board of Directors	20th Sep 2022	Annually Reviewed
1.4	27th April 2023	Mr. Chandrashekar Chettiar and Mr. Pankaj Purohit	Board of Directors	27th April 2023	Annually Reviewed
1.5	26th April 2024	Mr. Chandrashekar Chettiar and Mr. Pankaj Purohit	Board of Directors	26th April 2024	Bi-annually
1.6	25th June 2024	Mr. Chandrashekar Chettiar	Cybersecurity Committee	25th June 2024	Incorporate NSE QSB comments
1.7	28th Oct 2024	Mr. Chandrashekar Chettiar	Board of directors	28th Oct 2024	Bi-annual Review
1.8	25th April 2025	Mr. Chandrashekar Chettiar	Board of directors	25th April 2025	Bi-annual Review

Contents

1. Introduction

The malicious use of information and communication technologies (ICT) could disrupt financial services crucial to both national and international financial systems, undermine security and confidence, and endanger financial stability. With the increase in the frequency, severity, and sophistication of cyber incidents in recent years, several legislative, regulatory, and supervisory initiatives have been taken to increase cyber resilience.

Cyber resilience is preparing for, responding to, and recovering from cyber-attacks. Cyber resilience which defines as the ability of an organization to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing, and rapidly recovering from cyber incidents. It helps MOFSL to protect against cyber risks, defend against and limit the severity of attacks, and ensure its continued survival despite an attack.

Cyber resilience refers to the ability of MOFSL to maintain its main business goals and integrity against the latest threat of cyber security attacks. As a cyber-resilient organization MOFSL can prevent, detect, contain, and recover, minimizing exposure to an attack and its impact on business, against countless threats to data, applications, and IT infrastructure and devices classified as MOFSL most valuable assets.

2. Scope

This policy mainly focuses on cyber resilience, but practices relevant to the broader operational resilience context are also considered. Cyber-risk management (which deals with vulnerabilities and threats) and IT risk management, and practices that reflect new approaches or address widely shared strategic concerns are also considered in the scope.

The scope also includes Resilience Management and Measurement for managing operational resilience which considers people, information, technology, and facilities as assets that support MOFSL services and measuring MOFSL capacities and capabilities in performing, planning, managing, measuring, and defining cyber security capabilities across:

1. Asset Management
2. Controls Management
3. Configuration and Change Management
4. Vulnerability Management
5. Incident Management
6. Service Continuity Management
7. Risk Management
8. External Dependency Management
9. Training and Awareness
10. Situational Awareness

3. Cyber-resilience standards and guidelines

Cyber-resilience requirements are embedded within high-level IT risk guidance which covers a wide range of regulatory standards. Guidance typically addresses governance, risk management, information security, IT recovery, and management of IT outsourcing arrangements. Standards on general risk topics such as business continuity planning and outsourcing contribute to managing a wide range of risks and are relevant to cyber risk. Key concepts from international and industry standards such as NIST, ISO/IEC, and regulator's guidelines are referred to for creating a cyber resilience framework which primarily includes detect, identify, protect, recover, and respond stages.

4. Cyber-Governance

The regulators have issued regulatory standards that address enterprise IT risk management that cover cyber-risk management of critical business functions, interconnectedness, or third-party risk management. Based on that following areas are identified and analyzed relevant to governance :

4.1 Cyber Security Strategy

MOFSL shall have a board-approved information security strategy in compliance with principles-based risk management practices, Information security strategy, information security plans, and cyber-security implementation, including key cyber-security initiatives and timelines policy and procedures under the broad remit of effective oversight of technology. Regulators review these strategies as part of their assessment of MOFSL's overall risk management practices.

4.2 Management roles and responsibilities

MOFSL understands the importance of the board of directors (BoD) and senior management's roles and responsibilities in cyber governance and controls to achieve cyber resilience.

MOFSL shall seek inputs from the cybersecurity committee while framing policies relating to establishing a robust cybersecurity framework and augmenting IT infrastructure and scalability of operations. The cyber security committee of the MOFSL will conduct bi-annual reviews of the framework and analyze any cyber-attack incidents to enhance the MOFSL cyber security measures.

The Cybersecurity Committee Includes

- Head Information Technology (IT), Chairman
- Senior group vice president, IT Infrastructure
- Chief Information security Officer (CISO)
- Executive Group Vice President, Operations
- Independent cyber security advisor

For effective implementation across functional teams representing but not limited to Governance, Business Operations, IT Security Planning and Management, Business Continuity and Disaster Recovery Planning, IT Infrastructure, Risk Management, IT Operations and Procurement, and Vendor Management, including those responsible for the functions to achieve cyber resilience.

4.3 Cyber risk awareness culture

Awareness of cyber risk at MOFSL emphasizes the importance of risk awareness and risk culture for staff and management at all levels, including BoDs and third-party employees. Increasing cyber-security awareness and a common risk culture across MOFSL are prerequisites for maintaining cyber-resilience. Regulators in most jurisdictions have published guidance emphasizing the importance of risk awareness and risk culture for staff and management at all levels, including BoDs and third-party employees. MOFSL shall provide cyber-security awareness training during each phase of the employment process, from recruitment to termination.

To mitigate insider threats, MOFSL shall have employees complete a screening and background verification process. MOFSL shall have robust processes and controls in place to ensure their employees, contractors and third-party vendors understand their responsibilities, are suitable for their roles, and have the requisite skills to reduce the risk of theft, fraud, or misuse of facilities. MOFSL shall have the development of a common risk culture sufficient to ensure effective cyber-risk management considering such factors as MOFSL's business model, core business strategy, and key technologies. MOFSL views cyber-security as a critical business function since a cyber-attack could lead to the insolvency of individual entities or even to widespread disruption of MOFSL services.

4.4 Architecture and Standards

MOFSL shall place controls and substantial supervisory guidance for cyber-security architecture and network architecture.

MOFSL shall confirm that the cyber-security architecture and network architecture diagrams are current, securely stored and reflective of a defense-in-depth security architecture and are subject to periodic assessment and updation.

4.5 Cyber-security workforce

MOFSL shall develop policy and procedures that address the responsibilities of the IT workforce and information security functions, with particular attention to cyber-security training and competencies to address cyber-security workforce skill set and dedicated frameworks to upgrade cyber-workforce skills and competencies.

4.6 Cyber Capability Index (CCI)

MOFSL shall conduct self assessment of their cyber resilience using CCI on a yearly basis to assess their cyber resilience posture.

5. Cyber security and cyber resilience framework

The cyber security and resilience framework is built around five main areas:

5.1 Identity

- Critical systems shall be identified based on their confidentiality and criticality for business operations, services, and data management. The critical systems 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 to access, control access, and communicate with critical systems either for operations or maintenance shall also be classified as critical systems.
- The technology team shall maintain an up-to-date inventory of critical systems (hardware and systems, software and information assets (internal and external)) along with interfaces, network resources, connections to its network, and data flows.
- Cyber risks (threats and vulnerabilities) shall be identified, along with the likelihood of such threats and impact on the business, and thereby, deploy controls commensurate to the criticality.
- MOFSL’s third-party engagements shall be encouraged to have similar security standards.

5.2 Protect

5.2.1 Access Control

- Access to MOFSL's critical systems shall follow a role-based approach for business purposes.
- Access to MOFSL's critical systems shall be for business purposes based on the individual's role.
- Access shall be granted to IT systems, applications, databases, and networks on a need-to-use basis and based on the principle of least privilege. Such access shall be for the period when the access is required and shall be authorized using strong authentication mechanisms.
- Adequate password controls shall be implemented for users' access to systems, applications, networks, and databases.
- The user credential data shall be stored using secure hashing algorithms.
- All privileged user access shall be supervised using adequate privilege management.
- MOFSL employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to critical systems, networks, and other computer resources, shall be subject to supervision, monitoring, and access restrictions.
- All users that connect to MOFSL's critical systems over the internet will be authenticated using 2-factor authentication schemes.
- MOFSL shall monitor and regulate the use of internet and internet-based services of its users.
- A proper 'end of life' mechanism should be adopted to deactivate access privileges of users of critical systems, who are leaving the organization or whose access privileges have been withdrawn.
- Deactivation of access privileges of users who are leaving the organization or whose access privileges have been withdrawn shall be managed through appropriate off-boarding/ "end of life" process.

5.2.2 Internet security:

To outline the guidelines for users for the acceptable usage of MOFSL internet facilities and services. MOFSL internet services shall be used for business, educational, and research purposes only. Usage of internet services at MOFSL is subject to monitoring by the applicability of law and MOFSL's policies.

Users should not use internet facilities to:

- Download or distribute malicious software or tools or deliberately propagate any virus and malware.
- Violate any copyright or license agreement by downloading or distributing protected material or pirated software.
- Share and upload any confidential or sensitive information of the organization or software without adequate authorization.
- Post any organization's proprietary and sensitive information or customer's sensitive proprietary and sensitive information on internet share drives, public forums, newsrooms, or bulletin boards.
- Post remarks that are defamatory, obscene, or may harm/tarnish the image, reputation and/or goodwill of the organization and/or any of its personnel on social media.
- Conduct illegal or unethical activities including gambling, accessing obscene material, or misrepresenting the organization.
- Users, therefore, shall exercise extreme caution in using the internet for their personal use.

5.2.3 Physical Security

Physical protection of personnel and property in information-processing facilities that house critical information assets from environmental and man-made threats is of prime importance to MOFSL. This shall be achieved by developing and implementing appropriate security controls.

Refer Information Security Policy and Procedures (MOFSL/POL/002/InfoSec)

5.2.4 Data Security

- MOFSL shall install network security devices, such as firewalls, proxy servers, and intrusion detection and prevention systems (IDS/IPS) to protect their IT infrastructure which is exposed to the internet, from security exposures originating from internal and external sources.

- Adequate controls shall 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.
- Critical data shall be identified and encrypted in motion and at rest by using strong encryption methods.
- MOFSL shall implement measures to prevent unauthorized access or copying, or transmission of data / information held in contractual or fiduciary capacity. It shall be ensured that the confidentiality of information is not compromised during the process of exchanging and transferring information with external parties.

5.2.5 Hardening of Hardware and Software

- Only hardened and vetted hardware/software shall be deployed within the production environment of MOFSL.
- Services shall be enabled on critical systems based on business requirements.

5.2.6 Application Security and Testing

- Application Security testing shall be carried out for new or modified critical systems before they are deployed into the production environment.
- Scope of testing shall at the least cover business logic security controls and system performance under various stress-load scenarios and recovery conditions.
- A patch management process shall be implemented to ensure the identification, categorization, and prioritization of security patches for all systems as per an implementation timeframe for each patch category.
- Adequate testing of patches shall be carried out before deploying them in the production environment.

5.2.7 Disposal of systems and storage devices

- Appropriate secure disposal policy shall be maintained for secure disposal of storage media and systems secure disposal shall be carried out for disposing of systems and information.

  Refer to Information Security Policies and Procedures

5.2.8 Data Retention and Archival Policy

The Data Retention Policy at MOFSL ensures that data is retained for appropriate periods to comply with business, legal, and regulatory requirements. Data must be securely stored throughout its retention period and properly disposed of once it is no longer necessary. The policy is reviewed annually to ensure alignment with current regulations and business needs.

Refer to Information Security Policy and Procedures

5.2.9 Vulnerability Assessment and Penetration Testing (VAPT)

- Bi-annually vulnerability assessment shall be carried out for critical and supporting systems to detect security vulnerabilities.
- Before launching a new accessible system, ensuring its security through comprehensive vulnerability scanning and penetration testing will be done by MOFSL. This approach identifies and mitigates potential security risks.
- A penetration test shall be carried out for critical systems at least Bi-annually and the output of the test shall be reported formally to the Technology & Cyber security committee.
- Identified vulnerabilities shall be addressed with adequate remedial actions within a stipulated time. Vulnerabilities shall be identified before the commissioning of new systems that are accessible over MOFSL's network interfaces.

5.2.10 Monitoring System

- MOFSL shall maintain a Security Operations Center (SOC) equipped with Security Information and Event Management (SIEM) tools to continuously monitor and analyze logs and network traffic for signs of unauthorized or malicious activities.

- The SOC shall promptly detect and respond to suspicious activities identified through SIEM alerts and other monitoring mechanisms and provide CISO with required information directly from source systems during IS reviews. Incident response procedures *(refer Incident Management Policy MOFSL/POL/012/Incident***)** shall be documented and regularly reviewed to ensure effectiveness.
- MOFSL shall adhere to logging and retention standards defined by regulatory requirements and best practices. Logs generated by systems, applications, and network devices shall be stored securely and retained for a specified period to facilitate forensic analysis and compliance audits.
- The Web Application Firewall (WAF) and IDS/IPS shall be configured to monitor network traffic and web application activities in real-time. Alerts generated by these systems indicating suspicious or unauthorized access attempts shall be promptly investigated and responded to by designated security personnel.

5.3 Detect

MOFSL shall set up both proactive and detective mechanisms to detect any potential activities which may lead to any security events or incidents. A Security Operations Center (SOC) / SIEM shall been set up for the detection of incidents, anomalies, and attacks by log correlation and analysis. IT Security team shall ensure that regular vulnerability assessment testing and audits are conducted in order to detect known attacks. Incident response shall be based on the incident management process documented as part of the Information Security Policy and Procedures (***POL-IT-004-24-Information Security Policy and Procedures)*.**

5.4 Respond

MOFSL shall develop and maintain an incident management process to resolve security incidents. Information Security Team along with the relevant stakeholders shall identify the incident and implement the necessary controls to resolve the incident.

5.5 Recover

Information Security team shall ensure that there are adequate mechanisms for identification and testing of contingencies towards the critical systems and timely recovery of the systems to normal operation as per the defined RTO and RPO in the Business Continuity and Disaster Recovery Plan document. The recovery and preventive measures shall be discussed and communicated to all the relevant entities in MOFSL.

5.6 Evolve

A major component of cyber resilience is the ability to adapt and improve the security posture to stay ahead of threats.

- MOFSL shall formulate strategies to anticipate new attack vectors by removing or applying new controls to compensate for identified vulnerabilities or weaknesses, reducing or manipulating attack surfaces, and proactively orienting controls, practices, and capabilities to prospective, emerging, or potential threats.
- MOFSL shall demonstrate heterogeneity to minimize common mode failures, particularly threat events exploiting common vulnerabilities.
- MOFSL shall confirm post-incident modification of business functions and supporting processes to handle adversity and address environmental changes more effectively. In case of a cybersecurity incident, learning shall be incorporated to improve and evolve their cyber resilience posture.
- MOFSL shall continuously adapt and evolve to counter new cybersecurity threats and challenges and shall periodically evaluate their cyber resilience posture.

6. Approaches to risk management, testing incident response, and recovery.

MOFSL shall implement practices on cyber-risk management, and incident response and recovery which aims to identify practices in the supervision cyber-resilience at MOFSL, which includes:

- Methods for supervising cyber-resilience

- Information security controls testing and independent assurance
- Response and recovery testing and exercising
- Cyber-security and resilience metrics

6.1 Methods for supervising cyber-resilience.

- MOFSL shall have Risk specialists to assess information security management and controls which primarily focus on key risks such as cyber in the context of the scale, complexity of MOFSL's business model, and previous findings along with guidelines by regulators to maintain financial and operational resilience. In addition to this MOFSL shall have its risk assessments, findings from on-site inspections or questionnaires, and incidents (e.g. cyber incident trend analysis) and shall document evidence including risks, physical inspections, incident reports, and in-person meetings to assess the adequacy of controls in place.
- MOFSL's IT security team shall review information security controls to assess compliance with regulatory standards and alignment with good governing practices. These reviews focus on IT governance and strategy, management and frameworks, controls, third-party arrangements, training, monitoring and detection, response and recovery, and information-sharing and communication to achieve cyber resilience.

6.2 Information security controls testing and independent assurance.

- As a basis for building cyber resilience MOFSL shall develop mapping and classifying models for MOFSL business services and supporting assets and services. A clear understanding of business services and supporting assets (and their criticality and sensitivity) can be used to design testing and assurance of end-to-end business services. MOFSL shall have reports and documents of business impact analysis, recovery, and resolution planning, reviewing dependency of critical services on external third parties, monitoring, and surveillance of emerging threats, including real-time detection capability, ability to detect adversaries before they move between systems and relevant continuity and control policies for assessments.

- MOFSL shall have independent assurance from third parties which provides reports to management and regulators with an evaluation of whether appropriate controls have been implemented effectively and will typically test information security controls applied to hardware, software, and data to prevent, detect, respond, and recover from cyber-incidents for achieving cyber resilience.

6.3 Response and recovery testing and exercising

- MOFSL shall have business continuity plans focused on reviewing alignment with MOFSL risk management frameworks, the business continuity management strategies chosen, IT disaster recovery arrangements, and data center strategies and shall establish a framework or policy for prevention, detection, response and recovery activities, including incident reporting and shall have a prescribed cyber-incident response framework to be a key component of cyber-governance regarding incident management, covering identification of indicator of compromise, analysis and classification of events and escalation and reporting of incidents.
- MOFSL shall have incident response and recovery plans that focus on how plans are triggered, MOFSL's ability to implement plans, preservation of data, and specific actions for "critical" technology. (as defined in Technical Glitch SOP section 10 Capacity Planning)

6.4 Cyber-security and resilience metrics

MOFSL shall have methodologies approved by management to assess or benchmark MOFSL's cyber-security and resilience which provide information on building and ensuring cyber-security and resilience. Cyber resilience metrics track compliance with internal policies while others measure inherent risk. The state of cyber-resilience and operational resilience levels shall be reviewed by MOFSL regularly to assess its business needs and risk appetite.

1. Incident Metrics

   Number of Incidents: Total number of security incidents reported over a specific period.

Incident Response Time: Average time taken to detect, respond to, and resolve security incidents.

Incident Classification: Types and categories of incidents (e.g., malware, phishing, data breaches).

2. Vulnerability Metrics

   Number of Vulnerabilities: Total number of identified vulnerabilities in systems and applications.

   Vulnerability Remediation Time: Average time taken to patch or mitigate vulnerabilities after they are identified.

   Vulnerability Severity: Severity levels of vulnerabilities (e.g., critical, high, medium, low).

3. Compliance Metrics

   Total Audit Findings: Number of total audit findings

   Open Audit Findings: Number of open audit findings

   Closed Audit Findings: Number of closed audit findings

4. Risk Metrics

   Risk Assessment Results: Number and severity of risks identified during risk assessments.

   Risk Mitigation Effectiveness: Percentage of identified risks that have been mitigated or accepted.

5. User Awareness and Training Metrics

   Training Completion Rate: Percentage of employees who have completed cybersecurity awareness training.

   Phishing Simulation Results: A success rate of phishing simulations and employee response rates.

6. System and Network Metrics

   Patch Management: Percentage of systems with up-to-date patches and updates.

   System Downtime: Amount of time systems are down due to security incidents or maintenance.

The above mentioned cyber security and resilience metrics shall be maintained in Excel form and shared with CISO on a monthly basis for review.

7. Communication and sharing of information

MOFSL shall have information sharing mechanisms including cyber-threat information, information related to cyber-security incidents, regulatory and supervisory responses in case of cyber-security incidents and/or identifications of cyber-threat, and best practices related to cyber-security risk management which include public announcement/disclosure of information about cyber-security incidents and cross-sector information-sharing with public and private institutions.

8. Interconnections with third parties

Interconnections with third parties in the context of cyber security and cyber resilience shall adhere to stringent security protocols and regulatory requirements.

Prior to establishing any connection, a comprehensive risk assessment, including vulnerability testing and due diligence, shall be conducted. Implementing a strategy to distribute service provision across multiple vendors to lessen reliance on a single or limited number of vendors shall be put in place.

Formal agreements outlining roles, responsibilities, data protection measures, and incident response protocols shall be established to mitigate risks and ensure continuous protection of organizational assets.

9. Periodic Audit

- MOFSL and its implementation of control objectives, controls, policies, processes, and guidelines for information security, shall be reviewed independently periodically or when significant changes occur.
- The audit process shall comply with all applicable regulatory requirements. Audits shall be conducted bi-annually to meet the regulatory requirements.

Cyber Security & Cyber Resilience Audit Report shall be placed before the Cybersecurity / Technology Committee and observations identified, corrective action taken, and measures shall be taken to prevent recurrence of such observations.

10. Training

A dedicated program on cybersecurity, cyber resilience, and system hygiene shall bee made for Board members.

11. Review of the Policy

This Policy document is owned and managed by the Information Security Team of MOFSL. The same shall be approved by the Cybersecurity Committee / The Board of Directors Bi-anually.

12. Exceptions

Exceptions to this policy shall only be allowed with documentation and CISO written approval. If any exception must be made, CISO must approve and the same should be brought to the notice of the cybersecurity committee members.

13. Violations

Violations shall be met with a verbal or written acknowledgment of the violation. Committee Members shall determine if further action is to be taken.

14. Reference

14.1 SEBI Reference

- SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/24 (Enhanced obligations and responsibilities on Qualified Stock Brokers (QSBs), February 6 2023)
- SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113 (Cyber Security & Cyber Resilience Framework)

15. Cyber Security Incident Reporting Compliances and Penalties

Sr. No.	Compliances	Timeline for Reporting Compliance	Penalty
1	Cyber Security Incident to be reported to following entities and email Id's	Cyber Incident to be reported within 6 hours of noticing/detecting incidents or being brought to the notice about such incidents to the following entities CERTIN NCIIPC- Members, whose systems have been identified as "Protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC Ministry of Home Affairs (MHA) Cyber Security Cell of Police for further assistance on the reported Cyber Security incident Members shall submit details whether Cyber Security incident has been registered as a complaint with law enforcement agencies such as Police or its Cyber Security cell. Division Chiefs (in-charge of divisions at the time of submission) of DOS-MIRSD and CISO of SEBI	Exchanges directed to ensure compliance

		Email Id's of the entities where Cyber Incident to be reported within the timeline specified above 1. incident@cert-in.org.in 2. *sbdp-cyberincidents@sebi.gov.in*. BSE- through BEFS portal (Ask compliance for Login ID and Password https://befs.bseindia.com -> Cyber Incident Report> Immediate Incident Reporting. MCX- Infosec@mcxindia.com. NSE - compliance_wro@nse.co.in; compliance_assistance@nse.co.in; cybersecurityalerts@nse.co.in, Reporting on NSE portal NCDEX- askus@ncdex.com; infosec@ncdex.com CDSL- dpinfosec@cdslindia.com; helpdesk@cdslindia.com; Operations@cdslindia.com and direct upload in Audit Web NSDL - Participant-Interface@nsdl.co.in; dpinfosec@nsdl.co.in; DepCyberCompliance@nsdl.co.in	
2	Quarterly Reporting of Cyber Security Incident	Within 15 days from the end of the quarter.	
3	VAPT Audit to be conducted at least once in a Financial Year.	VAPT shall be completed during the period September to November of every financial year and the final report on said VAPT shall be submitted to the Stock Exchanges / Depositories	

	Engage CERT-In empaneled organizations for conducting VAPT	after approval from Technology Committee of respective Stock Brokers / Depository Participants, within 1 month of completion of VAPT activity. 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.	