Motilal Oswal Financial Service Limited

Cyber Security & Cyber Resilience Policy

Document identifier - MOFSL/POL/010/CyberResilience

Version number - 1.9

Effective date – 30th October 2025

Document Details

Sr No.	Type of Information	Document Data
	Document Title	Cybersecurity and Cyber Resilience Policy
2.	Document Version	1.9
3.	Date of Release	30th October 2025
4.	First Published Date	11th May 2019
5	Classification	Confidential
6.	Document Owner	CISO
7.	Document Author	CISO
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
1.9	30th October 2025	Mr. Suresh Sharma & Mr. Chandrashekar Chettiar	Board of directors	30th October 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. To ensure the goal of cybersecurity, MOFSL shall define responsibilities of its own employees, third-party service providers' employees, and other entities, who may have privileged access or use their systems/ networks.

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 National Institute of Standards and Technology (NIST), International Organization for Standardization (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.

The cybersecurity policy shall encompass the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organisation (NTRO), GoI in the report titled 'Guidelines for Protection of National Critical Information Infrastructure' and subsequent revisions, if any, from time to time.

MOFSL shall understand, manage and comply with relevant cybersecurity and data security/ protection requirements mentioned in government guidelines/ policies/ laws/ circulars/ regulations, etc. issued by SEBI/ GoI such as IT Act 2000, Digital Personal Data Protection Act (DPDP) 2023 or any other law/ circular/ regulation as and when issued.

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 information security strategy in compliance with principles-based risk management practices, 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.

Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.

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
- Head, IT Infrastructure
- Chief Information security Officer (CISO)
- Head, Operations
- Independent cyber security advisor

The Cyber Secuity committee and the senior management of MOFSL , including the CISO, shall periodically review instances of cybersecurity incidents/ attacks, if any, domestically and globally, and take steps to strengthen cybersecurity and cyber resilience.

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.

MOFSL shall devise SOPs to implement the advisories issued by CERT-In, NCIIPC or any other government agency in their IT environment within a defined timeframe.Aditionally, MOFSL shall establish a reporting procedure to facilitate communication of cybersecurity incidents/ unusual activities to the CISO or to the senior management in a time-bound manner as defined by guidelines/ policies/ laws/ circulars/ regulations, etc.

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.

MOFSL shall and self-assessment of their cyber resilience using CCI and submit corresponding evidences to their submission authority on a periodic basis.

MOFSL shall strive for building an automated tool and suitable dashboards (preferably integrated with log aggregator) for submitting compliance of CCI. A dashboard shall be available at the time of cyber audit, onsite inspection/ audit by SEBI or any agency appointed by SEBI.

5. Cyber Security and Cyber Resilience Framework

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

5.1 Identify

- 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. Any additions/ deletions or changes in existing assets shall be reflected in the asset inventory within 3 working days.
- 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.

MOFSL shall follow the latest version of CIS Controls or equivalent standards which are prioritized set of safeguards and actions for cyber defense and provide specific and actionable ways to mitigate prevalent cybersecurity incidents/ attacks.

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.

  Refer Section 16 Access Control of Information Security Policy and Procedures (MOFSL/POL/002/InfoSec)
- MOFSL shall ensure proper remote access policy framework incorporating the specific requirements of accessing the enterprise resources (located in the data centre) securely from home using internet connection.

  Refer section 36.3 Remote Access Policy of Information Security Policy and Procedures (MOFSL/POL/002/InfoSec)

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.

Refer Section 21.1.1 Internet Security of Information Security Policy and Procedures (MOFSL/POL/002/InfoSec)

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 Section 19 Physical and Environmental Security of 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.
- MOFSL shall manager, understand and adhere to data security standards and guidelines and other government guidelines/ policies/ laws/ circulars/ regulations, etc. issued by SEBI/ GoI such as IT Act 2000, Digital Personal Data Protection Act (DPDP) 2023 or any other law/ circular/ regulation as and when issued.

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.
- MOFSL shall explore the feasibility of deploying diverse operating systems to reduce the risk of common vulnerabilities. Attack or compromise on one type of OS may not affect other OS deployed.

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. *Refer Section 35 Patch Management of Information Security Policy and Procedures (MOFSL/POL/002/InfoSec)*

- Adequate testing of patches shall be carried out before deploying them in the production environment.
- MOFSL shall prepare SOPs for open source application security and concerns from emerging technologies like Generative AI security.

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 Section 33 Assets Disposal of Information Security policy and Procedures (MOFSL/POL/002/InfoSec)

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 Section 32.4 Data Retention and Archival of Information Security Policy and Procedures

(MOFSL/POL/002/InfoSec)

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.
- MOFSL shall perform VAPT prior to the commissioning of new systems, especially those which are part of critical systems or connected to critical systems.
- Revalidation of VAPT post closure of observations shall be done in a time bound manner to ensure that all the open vulnerabilities have been fixed.

- In case of vulnerabilities being discovered in COTS (used for core business) or empaneled applications, MOFSL shall report them to the vendors and the designated stock exchanges and/ or depositories in a timely manner.

  Refer Vulnerability Assessment and Penetration Testing SOP (MOFSL/SOP/018/VAPT)

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 root- cause analysis and compliance audits.
- The Web Application Firewall (WAF) and Intrusion Detection System (IDS)/Intrusion Prevention System (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.
- MOFSL shall use auditing/logging systems on different operating systems to acquire and store audit/logging data.
- To include heterogeneity, MOFSL shall apply different audit/logging regimes at different architectural layers.

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 *(MOFSL/POL/002/InfoSec)*.

MOFSL shall have processes in place to manage and incorporate IOAs/ IOCs/ malware alerts/ vulnerability alerts (received from CERT-In or NCIIPC (as applicable) or any other government agencies) in their systems.

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 Recovery Time Objective (RTO) and Recovery Point Objective (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.

Recovery plans shall be discussed with the IT Committee. These plans shall include coordination with relevant stakeholders during the recovery process and define both internal and external communication protocols.

Refer BCP-DR Policy (MOFSL/POL/004/BCP-DR)

Additionally, an indicative (but not exhaustive and limited to) recovery plan to be followed by MOFSL has been attached at Annexure A.

Furthermore, while ensuring protection of data and security of processes, MOFSL's BCP-DR capabilities shall support its cyber resilience objectives, enabling rapid recovery and resumption of critical operations following a cybersecurity incident.

A backup and recovery plan shall be formulated by MOFSL and approved by its IT Committee. The backup and recovery plan shall include policies and software solutions that work together

to maintain business continuity in the event of a security incident. Such plan shall include guidance on restoration of data with the backup software used by MOFSL.

- The backup and recovery policy shall include backup of data as well as backup of server images to ensure complete restoration capability.
- The backup of data and server images shall be maintained at off-site locations to keep backup copies intact and unbroken.
- Recovery Time Objective (RTO) and Recovery Point Objective (RPO), as prescribed by SEBI from time to time, shall be included in the recovery plan for the restoration of systems after cybersecurity incidents.
- MOFSL shall maintain offline, encrypted backups of data and shall regularly test these backups at least on a quarterly basis to ensure confidentiality, integrity, and availability of data.
- To further strengthen recovery capabilities, MOFSL shall ensure that Recovery Time Objectives (RTOs) for all interconnected systems and networks are consistently met through capacity upgradations and periodic coordinated resilience testing. Additionally, recovery plans shall be continuously improved by analyzing the learnings derived from periodic drills.

In addition to the above, MOFSL shall:

- Maintain regularly updated 'golden images' of critical systems at offsite location for rebuilding the systems (whenever required). This entails maintaining images "templates" that include a preconfigured operating system (OS), configuration setting backup and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server.
- Explore the possibility of retaining spare hardware in an isolated environment to rebuild systems in an event that starting MOFSL's operations from PDC and/ or DRS is not feasible. MOFSL shall also try to keep spare hardware in ready-to-use state for delivering critical services and such systems shall be updated as and when new changes (for example OS patches, security patches, etc.) are implemented in the primary systems. This spare hardware shall regularly undergo testing in-line with the response and recovery plan of MOFSL.
- Take necessary precautions while updating golden images and data backups to ensure their integrity and usability during recovery.

- In case of ransomware attacks that specifically target backups, conventional data backups may not be effective. Therefore, MOFSL shall create backups in an isolated and immutable (and/ or air-gapped) manner to ensure recovery if the production system is compromised.
- MOFSL shall undertake regular business continuity drills to check the readiness of the organization and effectiveness of existing security controls at the ground level. One such drill scenario recommended to be tested is recovering from a ransomware attack considering both PDC and DRS have been impacted. This shall assess the effectiveness of people, processes, and technologies to deal with such attacks.

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.
- MOFSL shall anticipate new attack vectors through threat modelling (based on risk assessment) and work to defend them.
- MOFSL shall strive for reducing its attack surfaces.
- MOFSL shall proactively examine controls, practices, and capabilities for prospective, emerging or potential threats.
- MOFSL shall proactively assess and take necessary actions with respect to its system's requirements, architecture, design, configuration, acquisition processes, or operational processes as a strategy for adaptation to the identified and prospective threats and vulnerabilities.

- MOFSL shall continuously improve upon the ability to quickly deploy and integrate existing and new services, both on-premises and in the cloud.
- MOFSL shall strive to rapidly correlate data using mathematical models and machine learning in order to make data-driven decisions.
- MOFSL shall maintain extra capacity of IT assets for information storage, processing, or communications.

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.
- As part of compliance management with respect to CSCRF, MOFSL shall apply following key aspects (including but not limited to) for implementing compliance management:
    a. Assess Compliance with applicable guidelines/ policies/ laws/ circulars/ regulations, etc. issued by SEBI or GoI.

b. Develop compliance policies and procedures. *Refer Cybersecurity Cyber Resilience Policy (MOFSL/POL/010/Cyber Security & Cyber Resilience)*

c. Implement controls such as security measures

d. Train employees

e. Monitor and review compliance management processes

f. Regular audits and reporting.

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.
- MOFSL shall follow Plan-Do-Check-Act concept while creating and using the documented information. For example, activities under the 'Plan' phase shall be guided by Policies, the 'Do' phase will follow Procedures (SOPs), and the 'Check' and 'Act' phases will refer to the Policies and Procedures.

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. (refer Risk Management Procedure section 8.3.4 Identification of Services and Assets *MOFSL/SOP/016/Risk*)
- Comprehensive scenario-based testing shall be done for assessing cybersecurity risks of MOFSL. MOFSL shall prepare their own attack scenarios as per their business model and assess their risks accordingly.
- MOFSL shall conduct suitable periodic drills to test the adequacy and effectiveness of its response and recovery plans.
- The updates and changes in the contingency plan, COOP, training exercises, and incident response and recovery plan shall be communicated and approved by the Board/ Partners/ Proprietor.
  - MOFSL shall periodically review and update its contingency plan, COOP, training exercises, and incident response and recovery plans (including the Cyber Crisis Management Plan – CCMP) to incorporate lessons learned and strengthen its response capabilities in the event of a future incident or attack.
  - Following any cybersecurity incident, MOFSL shall update its response and recovery plans (including CCMP) to improve cyber resilience and incorporate the learnings from the incident.

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.

In addition, MOFSL shall:

1. Notify SEBI and CERT-In within 6 hours of noticing/detecting any cyber-attack, cybersecurity incident, and/or breach falling under CERT-In Cybersecurity directions, or being informed about such incidents. This information shall be shared with SEBI via mkt_incidents@sebi.gov.in within 6 hours, and detailed incident information shall be reported on the SEBI Incident Reporting Portal within 24 hours. MOFSL shall also report the incidents to Stock Exchanges/Depositories along with SEBI and CERT-In within the same timeframe. All other cybersecurity incidents shall be reported to SEBI, CERT-In, and NCIIPC (as applicable) within 24 hours.

2. Share Threat Intelligence data that is collected, processed, and analyzed to gain insights into the motives and behavior of the threat actor, target, attack pattern, etc., on the SEBI Incident Reporting Portal.

3. Report incidents to CERT-In in accordance with the guidelines/directions issued by CERT-In from time to time. Additionally, if MOFSL's systems are identified as "Protected Systems" by NCIIPC, such incidents shall also be reported to NCIIPC.

4. Submit quarterly reports containing information on cyber-attacks, threats, cybersecurity incidents, and breaches experienced, along with measures taken to mitigate vulnerabilities, threats, and attacks. These reports shall include information on bugs/vulnerabilities and threats that may be useful for other entities and SEBI, and shall be submitted within 15 days from the end of each quarter (June, September, December, and March).

5. Share details deemed useful for other entities in a masked manner, using mechanisms specified by SEBI from time to time. While sharing sensitive information, MOFSL shall follow the Traffic Light Protocol (TLP) with four levels of sensitivity: white, green, amber, or red.

6. Provide regular reports to SEBI during the processing of reported incidents, including Root Cause Analysis (RCA), forensic analysis reports, and other relevant updates on the progress of incident analysis.

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.

All information/ data (classified as Regulatory Data and IT and Cybersecurity Data) that is consumed/ handled by MOFSL shall be made accessible to SEBI when required. If there is any dependency on external party, MOFSL shall facilitate information sharing with SEBI by including it in their agreement with external party.

SEBI circulars on outsourcing of activities, currently mandated and updated from time to time, shall be complied with by MOFSL.

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.
- The details of periodicity, timeline and report submission for cyber audit by MOFSL have been provided in the 'CSCRF Compliance, Audit Report Submission, and Timelines section.
- MOFSL shall regularly conduct cybersecurity audit and VAPT with scope as mentioned in CSCRF in order to detect vulnerabilities in the IT environment. Further, MOFSL shall conduct in-depth evaluation of the security posture of the system through simulations of actual attacks. An indicative (but not exhaustive and limited to) VAPT scope has been attached at Annexure-C: VAPT Scope.
- The assets under these audits shall include (but not limited to) all critical systems, infrastructure components (like networking systems, security devices, load balancers, servers, databases,

applications, remote access points, systems accessible through WAN, LAN as well as with Public IP's, websites, etc.), and other IT systems pertaining to the operations of MOFSL.

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)

Annexure A: Recovery Plan Template

1	Cybersecurity incident recovery plan	i. Preparation: Measures taken in preparation for cybersecurity incident (pre-incident).	
		ii. Identification Checklist	a. Source (Who has discovered or

			reported the incident?)
			b. When it was discovered?
			c. Details of the incident
			d. Incident occurred on on-prem/ cloud resource?
			e. What is the location (PDC/ DR/ Near DR, etc.) of the incident?
			f. The impact of the incident on the business operations
			g. What is the extent of the incident w.r.t applications and networks?
			h. Type of the incident (e.g. Phishing mail, weak credentials, ransomware attack, data breach, etc.)
			i. How did the Cybersecurity Incident occur?
		iii. Containment checklist	a. Can the incident be isolated to identify the scope of the incident and determine what systems, services, data or networks are compromised? If so,

			what are the steps taken, if not, explain why it can't be isolated?
			b. Are the affected systems kept isolated from the non-affected ones?
			c. Have the 'golden' server images and data been identified?
			d. Is the latest data backup (as per prescribed RPO) available?
			e. Have the copies of the infected machines preserved for digital forensics and incident response experts for analysis?
			f. Has the threat been removed from the infected devices?
		iv. Resolution checklist	Resolving the cause of the incident: a. Removing malware, b. Patching vulnerabilities, c. Taking other measures etc. Please specify resolution method
		v. Recovery checklist	a. Recover lost or corrupted data, b. Restore normal operations by returning systems and

			networks to a known good state c. Taking other measures etc.
2	Cybersecurity incident recovery plan scenarios		
3	Categorization of incidents		
4	Key assumptions and pre-requisites		
5	Authorization		
6	Details of the Incident Response Team (IRT) (Internal/External)		
7	Details of other teams involved (Internal/External)		
8	Cybersecurity incident recovery invocation		
9	Off site location address where 'golden' copy of server images and data are stored		
10	Recover System(s) and Services		
11	Recovery Actions		
12	Lessons learned: Document lessons learned from the incident and incorporate them into incident response and recovery plans.		
13	Post-incident: Measures taken to avoid reoccurrence of the cyber incident		
14	Perform Hotwash		

Annexure B: Cyber Capability Index (CCI)

REPORTING FORMAT FOR MIIs AND QUALIFIED REs TO SUBMIT THEIR CCI SCORE

NAME OF THE ORGANISATION: <Name>

ENTITY TYPE: <Intermediary Type>

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

RATIONALE FOR THE CATEGORY: <>

PERIOD: <>

NAME OF THE AUDITING ORGANISATION (applicable for MIIs): <Name>

MOFSL's Authorised signatory declaration:

I/ We hereby confirm that Cyber Capability Index (CCI) has been verified by me/ us and I/ We shall take the responsibility and ownership of the CCI report.

Signature:

Name of the signatory:

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

Company stamp:

Cyber Capability Index (CCI)
A. Background-

CCI is an index-framework to rate the preparedness and resilience of the cybersecurity framework of the Market Infrastructure Institutions (MIIs) and Qualified REs. MOFSL are directed to conduct self-assessment of their cyber resilience on an annual basis.

B. Index Calculation Methodology-

1. The index is calculated on the basis of 23 parameters. These parameters have been given different weightages.

2. Implementation evidence to be submitted to SEBI only on demand.

3. All implementation evidences shall be verified by the auditor for conducting third-party assessment of MIIs.

4. The list of CCI parameters, their corresponding target and weightages in the index, is as follows:

S.No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score
1.	Security Budget Measure **[GV.RR.S4]**	Information Security Goal: Provide resources necessary for information systems.	Percentage (%) of the organisation's information system budget devoted to information security.	Impact	(Information security budget/ total organisation's information technology budget) ×100	10%	1. What is the total information security budget across all organization's systems? 2. What is the total information technology budget across all organization's systems? 3. Approval Document from Competent Authority for the same.	8%	
2.	Vulnerability Measure **[DE.CM.S5]**	Objective of this measure is to ensure that the vulnerabilities in organization's systems are identified and mitigated	Percentage of vulnerabilities mitigated pertaining to organization in a specified time frame.	Effectiveness Measure	(Number of vulnerabilities mitigated/ Number of vulnerabilities identified)×100	100%	1. Confirmation that VAPT is done by CERT-In empanelled IS auditing organization and as per the scope prescribed by SEBI 2. VAPT report and its closure report. 3. Time taken to close the identified vulnerabilities.	18%	
3.	Security Training Measure	Information Security Goal: Ensure that organization's	Percentage (%) of information system	Implementation	(Number of information system security personnel that	100%	1. Details of the training/ awareness sessions scheduled within the past 1 year. 2. Cyber audit observation	5%	

	[PR.AT.S1]	personnel are adequately trained to carry out their assigned information security-related duties and responsibilities	security personnel that have received security training within the past one years.		have completed security training within the past year/total number of information system security personnel) ×100		against Standard 1 mentioned in 'Protect: Awareness and Training' header in CSCRF Part-I and respective guidelines in Part-II.		
4.	Remote Access Control Measure [PR.AA.S12]	Information Security Goal: Restrict access to information, systems, and components to individuals or machines that have been authenticated and are identifiable, known and credible.	Percentage (%) of remote users logging through MFA.	Effectiveness	(Number of remote users logging through MFA/ total number of remote users) ×100	100%	1. Does the organization use automated tools to maintain an up-to-date record that identifies all remote access points? 2. How many remote access points exist in the organization's network? 3. Does the organisation employ IDS or IPS to monitor traffic traversing remote access points? 4. Does the organisation collect and review audit logs associated with all remote access points? 5. Evidence of users who are allowed remote access through MFA, validated through Firewall, AD, or any dedicated system. 6. Based on reviews of the incident database, IDS/ IPS logs and alerts, and/ or appropriate remote access point log files, how many access points have been used to gain unauthorized access within the reporting period?	2%	
5.	Audit Record Review Measure [DE.CM.S1]	Information Security Goal: Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, suspicious or abnormal activity.	Percentage (%) of critical systems integrated with SIEM.	Efficiency	(Number of critical systems integrated with SIEM tool/total number of critical systems) ×100	100%	1. Is logging activated on the system? 2. Does the organization have clearly defined criteria for what constitutes evidence of "suspicious or abnormal" activity within system audit logs? 3. For the reporting period, how many system audit logs have been reviewed for past six months for suspicious or abnormal activity.	2%	
6.	Configuration Changes Measure	Information Security Goal: Establish and	Percentage (%) approved and	Implementation	(Number of approved and implemented	100%	1. Does the organization manage configuration changes to information systems using	2%	

	[DE.CM.S5]	maintain baseline configuration and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	implemented configuration changes identified in the latest automated baseline configuration.		configuration changes identified in the latest automated baseline configuration/ total number of configuration changes identified through automated or manual scans) × 100		an organizationally approved process? 2. Does the organization use automated scanning to identify configuration changes that were implemented on its systems and networks? 3. If yes, how many configuration changes were identified through automated scanning over the last reporting period? 4. How many change control requests were approved and implemented over the last reporting period? 5. Cyber audit observation against Standard 3 mentioned in 'Detect: Continuous Security Monitoring' header in CSCRF Part-I and respective guidelines in Part-II.		
7.	Contingency Plan Testing Measure [RS.MA.S3]	Information Security Goal: Establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery of organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.	Percentage (%) of information systems that have conducted contingency plan testing at least once in a year.	Effectiveness	(Number of information systems that have conducted contingency plans testing at least once in a year/ number of information systems in the system inventory) ×100	100%	1. How many information systems are in the system inventory? 2. How many information systems have an approved contingency plan? 3. How many contingency plans were successfully tested within the past 1 year? 4. Reports of the contingency plan testing conducted in past one year.	4%	
8.	User Accounts Measure [PR.AA.S7]	Information Security Goal: All privilege users are identified and authenticated in accordance with information security policy.	Percentage (%) of privileged access through PIM.	Effectiveness	(Number of systems accessed through PIM/ total number of systems) ×100	100%	1. Organization should have a documented and approved access control policy for systems, applications, networks, databases etc. 2. How many users have access to the system? 3. How many users have access to shared accounts? 4. Cyber audit observation against Standard 7 mentioned in 'Protect: Identity Management, Authentication, and Access Control' header in	3%	

							CSCRF Part-I and respective guidelines in Part-II.		
9.	Incident Response Measure [RS.CO. S2]	Information Security Goal: Track, document, and report incidents to appropriate organizational officials and/or authorities.	Percentage (%) of incidents reported within required time frame.	Effectiveness	(number of incidents reported on time/ total number of reported incidents) ×100	100%	1. How many incidents were reported during the period? 2. Of the incidents reported, how many were reported within the prescribed time frame?	2%	
10.	Maintenance Measure [PR.MA. S1]	Information Security Goal: Perform periodic and timely maintenance on organizational information systems and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.	Percentage (%) of system components that undergo maintenance in accordance with planned maintenance schedules.	Efficiency	(Number of system components that undergo maintenance according to planned maintenance schedules/ total number of system components) ×100	100%	1. Does the system have a planned maintenance schedule? 2. How many components are contained within the system? 3. How many components underwent maintenance in accordance with the planned maintenance schedule?	5%	
11.	Media Sanitization Measure [PR.AA. S14]	Information Security Goal: Sanitize or destroy information system media before disposal or release for reuse.	Percentage (%) of media that passes sanitization procedures testing.	Effectiveness	(Number of media that passes sanitization procedures testing/total number of media disposed or released for reuse) × 100	100%	1.Policy/procedure for sanitizing media before it is discarded or reused. 2. Indicative proof that policy is being followed. 3. Cyber audit observation against Standard 14 mentioned in 'Protect: Identity Management, Authentication, and Access Control' header in CSCRF Part-I and respective guidelines in Part-II.	2%	
12.	Physical Security Incidents Measure [PR.AA. S10]	Information Security Goal: Integrate physical and information security protection mechanisms to ensure appropriate protection of the organization's information resources.	Percentage (%) of physical security incidents allowing unauthorized entry into facilities containing information systems.	Effectiveness	(Number of physical security incidents allowing unauthorized entry into facilities containing information systems/total number of physical security incidents) ×100	0%	1.Policy/procedure ensuring the secure physical access to critical systems? 2. How many physical security incidents occurred during the specified period? 3. How many of the physical security incidents allowed unauthorized entry into facilities containing information systems? 4. Cyber audit Observation against Standard 10 mentioned in 'Protect: Identity Management, Authentication, and Access Control' header in	1%	

							CSCRF Part-I and respective guidelines in Part-II.		
13.	Planning Measure [GV.RR. S5]	Information Security Goal: Develop, document, periodically update, and implement security measures for authorised access to the information systems of the organisation.	Percentage of employees who get authorized access to information systems only after they sign an acknowledge ment that they have read and understood confidentiality and integrity agreement.	Implemen tation	(Number of users who are granted system access after signing confidentiality and integrity agreement/total number of users who are granted system access) ×100	100%	1. How many users accessed the system? 2. How many users signed confidentiality and integrity agreement acknowledgements? 3. How many users have been granted access to the information system only after signing confidentiality and integrity agreement acknowledgements?	1%	
14.	Personne l Security Screenin g Measure [PR.AA. S10]	Information Security Goal: Ensure that individuals occupying positions of responsibility within organizations are trustworthy and meet established security criteria for those positions.	Percentage (%) of individuals screened before being granted access to organizational information and information systems.	Implemen tation	(Number of individuals screened/total number of individuals having access to organization's information and information systems) ×100	100%	1. How many individuals have been granted access to organizational information and information systems? 2. What is the number of individuals who have completed personnel screening?	1%	
15.	Risk Assessm ent Measure [ID.RA. S2]	Objective of this measure is to periodically assess the risk to organization's IT assets and operations. Cybersecurity risks to the organization's information systems, and assets are understood and assessed.	Percentage of organization's information systems, and assets covered under risk assessment.	Implemen tation Measure	(Number of organization's information systems, and assets covered under risk assessment/Tot al number of organization information systems, and assets) ×100	100%	1. Has the organization completed a cyber-risk assessment? 2. Cyber Audit observation against this Standard 2 mentioned in 'Identify: Risk Assessment' header in CSCRF Part-I and respective guidelines in Part-II.	5%	
16.	Service Acquisiti on Contract Measure [GV.SC. S3]	Information Security Goal: Ensure third-party providers employ adequate security measures to protect information, applications, and/or services outsourced by the organization.	Percentage (%) of system and service acquisition contracts that include security requirements and/or specifications.	Implemen tation	(Number of system and service acquisition contracts that include security requirements and specifications/ total number of system and service acquisition contracts) ×100	100%	1. How many active service acquisition contracts does the organization have? 2. How many active service acquisition contracts include security requirements and specifications? 3. How many contracts includes integration of systems with SOC technologies? 4. Whether the acquisition contract includes SLA for vulnerabilities closure and timely implementation of patches? 5. Contracts for adoption of Cloud includes implementation of 'security of the cloud' , etc.	3%	
17.	System and Commu nication Protectio n Measure	Information Security Goal: Allocate sufficient resources to adequately protect	Percentage of mobile computers and devices that perform all cryptographic operations.	Implemen tation	(Number of mobile computers and devices that perform all cryptographic operations/total	100%	1. How many mobile computers and devices are used in the organization? 2. How many mobile computers and devices employ cryptography? 3. How many mobile	1%	

	[PR.DS.S4]	electronic information infrastructure.			number of mobile computers and devices) ×100		computers and devices have cryptography implementation waivers?		
18.	Risk Management [GV.RM.S1, GV.RM.S2]	Based on risk appetite of the organization, cybersecurity risks are identified, analysed, evaluated, prioritized, responded, and monitored.	Percentage (%) of organization information systems, and assets covered under risk management.	Effectiveness	(Number of organization information systems, and assets covered under risk management/Total number of organization information systems, and assets) ×100	100%	1. Does organization have a cyber-risk management framework? 2. Has the organization established, communicated, and maintained its risk appetite and risk tolerance statements? 3. Has organization responded to risk observations based on its risk appetite?	8%	
19.	Critical Assets Identified [ID.AM.S1, ID.AM.S2]	Objective of this measure is to ensure identification and management of assets in accordance with their relative importance to the organizational objectives and the organization's risk strategy.	Percentage (%) of the critical systems identified by REs among all other IT systems.	Implementation Measure	(Number of critical systems Identified/ Total IT systems integrated with SOC) ×100	50%	1. Process to identify and approve the list of critical assets. 2. List of critical assets identified as per the ID.AM.S1. 3. Auditors reports on identification of assets as critical/ non-critical.	9%	
20.	CSK Events [RS.MA.S5]	Objective of this measure is to mitigate threats upon external IPs	Number of CSK reported events closed in timely manner.	Effectiveness Measure	(Total number of CSK reported events closed in 15 days/ Total number of CSK reported events to the organization)×100	100%	1. Summary report of the events reported by CSK.	4%	
21.	Cybersecurity Policy Document [GV.PO.S1]	Develop, document, periodically update, and implement cybersecurity policies and procedures for organizational information systems that describe the security controls in place or planned for information systems.			Non quantifiable measure		1. Cybersecurity Policy document of the organization. 2. Frequency of the revision of the policy document. 3. Approval of the policy document. 4. Cyber audit observation against Standard 1 mentioned in 'Governance: Policy' header in CSCRF Part-I and respective guidelines in Part-II.	4%	
22.	SOC efficacy	How effective is our SOC operational?	SOC efficacy score	Effectiveness	As specified in SOC efficacy (Annexure-N)	100%	1. How effective is the functioning of RE's SOC?	5%	
23.	Automated compliance with CSCRF	Develop an automated tool (preferably integrated with log aggregator) to submit compliance with CSCRF.	Percentage (%) of standards compliance automated	Maturity measure	(Number of standards for which compliance has been automated for CSCRF compliance/Total number of CSCRF standards)×100	100%	1. Automated dashboard to get detailed reports of CSCRF standards compliance.	5%	

5. Based on the value of the index, the cybersecurity maturity level of the MIIs and Qualified REs shall be determined as follows:

SN.	Rating	Index Score Rating
1	Exceptional Cybersecurity Maturity	100-91
2	Optimal Cybersecurity Maturity	90-81
3	Manageable Cybersecurity Maturity	80-71
4	Developing Cybersecurity Maturity	70-61
5	Bare Minimum Cybersecurity Maturity	60-51
6	Fail	< =50 (MOFSL has scored below the cut-off in at least one domain/ sub-domain)

6. MOFSL shall strive for building an automated tool and suitable dashboards (preferably integrated with log aggregator) for submitting compliance. A dashboard shall be available at the time of cyber audit, onsite inspection/ audit by SEBI or any agency appointed by SEBI.

Annexure C: VAPT Scope

Comprehensive Scope for Vulnerability Assessment and Penetration Testing (VAPT)

1. The scope of the IT environment taken for VAPT should be made transparent to SEBI and should include all critical assets and infrastructure components including (not limited to) Networking systems, Security devices, Servers, Databases, Applications, Systems accessible through WAN, LAN as well as with public IP's, websites, etc.

The scope should include (not limited to):

S. No.	VAPT scope
1.	VA of Infrastructure-Internal & External
2.	VA of Applications-Internal & External
3.	External Penetration Testing-Infrastructure & Application
4.	WIFI Testing
5.	API Security Testing
6.	Network Segmentation
7.	VA & PT of Mobile applications

8.	OS & DB Assessment
9.	VAPT of Cloud implementation and deployments
10.	Configuration audit

2. Testing methodology: The VAPT should provide in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks. The testing methodology should adapt from the following:

a. SEBI CSCRF
b. National Critical Information Infrastructure Protection Centre (NCIIPC)
c. CERT-In Guidelines
d. The National Institute of Standards and Technology ("NIST") Special Publication 800-115
e. Latest ISO27001
f. PCI-DSS standards
g. Open Source Security Testing Methodology Manual ("OSSTMM")
h. OWASP Testing Guide