Consultation Paper on Consolidated Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities

Version: 1.0

Date: July 04, 2023

Securities and Exchange Board of India

Plot no. C4-A, G Block, Bandra Kurla Complex,

Bandra (East), Mumbai – 400051, India

Tel.: +91-22-26449000/40459000

Website: www.sebi.gov.in

This page intentionally left blank

Executive Summary

Prevention of damage to, protection of, and restoration of computers, electronic communication systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. – **NIST SP 800-53**[1] cybersecurity definition.

The use of Information Technology has grown rapidly in securities market and has become a critical component of SEBI Regulated Entities (REs). However, with these swift technological advancements, protection of IT infrastructure and data through cybersecurity measures has become a key concern for SEBI and its REs. Since 2015, SEBI has issued various cybersecurity and cyber resilience frameworks to address cybersecurity risks and enhance cyber resilience for the SEBI REs. Further, SEBI has also issued an advisory on cybersecurity best practices for all the REs.

In order to enhance the scope of cybersecurity and cyber resilience framework, to address the need of uniformity of cybersecurity guidelines for all REs and to strengthen the mechanism to deal with cyber risks / threats / incidents, the master framework on cybersecurity and cyber resilience has been drafted after discussion with SEBI's High Powered Steering Committee - Cyber Security (HPSC-CS).

The framework provides a common structure for multiple approaches to cybersecurity to prevent any cyber-risks / incidents. The framework follows graded approach and divides the guidelines in three parts:

i. Applicable to all REs
ii. Applicable to specified REs[2]
iii. Applicable to Market Infrastructure Institutions (MIIs)[3].

The summary of the framework is as follows:

The framework is based on five concurrent and continuous functions of cybersecurity as defined by NIST – **Identify, Protect, Detect, Respond, and Recover**. It references globally recognized standards, e.g., NIST Special Publication 800-53 Revision 5, COBIT 5, and CIS controls for cybersecurity controls, outcomes, and guidance to achieve those outcomes.

[1] Refer NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information System and Organizations https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[2] Refer Definitions section for the specified REs criteria.

[3] Refer Definitions section for the MIIs definition.

Framework compliance reporting shall be done by REs to their respective authorities[4] in the standardized formats notified by SEBI. The format for VAPT reporting and Cyber audit reporting has been added.

i. **IDENTIFY**

a. REs shall identify and classify critical assets based on their sensitivity and criticality for business operations, services and data management. The Board / Partner / Proprietor of the REs shall approve the list of critical systems.

b. REs shall formulate a comprehensive cybersecurity and cyber resilience policy and incorporate best practices from standards such as ISO 27001, COBIT 5, etc.

c. Comprehensive scenario-based testing shall be done for assessing risk related to cybersecurity in REs' IT environment including both internal and external cyber-risks.

d. REs shall be solely accountable for all aspects related to third-party services taken including (but not limited to) confidentiality, integrity, availability, non-repudiation, and security of its data and logs, and ensuring compliance with laws, regulations, circulars, etc. issued by SEBI / Government of India. Accordingly, REs shall be responsible and accountable for any violation of the same.

ii. **PROTECT**

a. Strong log retention policy, password policy and access policy shall be documented and implemented.

b. REs shall implement network segmentation techniques to restrict access to the sensitive information, hosts, and services.

c. Layering of Full-disk Encryption (FDE) along with File-based Encryption (FE) shall be used for data protection.

d. For the development of all critical software / applications and further feature enhancements, there shall be separate Development, System Integration Testing, User Acceptance Testing and Quality Assurance environments.

e. Periodic audit shall be conducted by a CERT-In empanelled auditor to audit the implementation and compliance to standards mentioned in the consolidated CSCRF.

f. Vulnerability Assessment and Penetration Testing (VAPT) shall be done to detect open vulnerabilities in the IT environment for critical assets and infrastructure components as defined in the framework. A comprehensive VAPT scope has also been added.

g. Application Programming Interface (API) security and Endpoint security solution shall be implemented with rate limiting, throttling, and proper authentication and authorisation mechanisms.

[4] Refer Framework Compliance section.

h. Applicable to MIIs: ISO 27001 certification shall be mandatory for MIIs as it provides essential security standards with respect to Information Security Management System (ISMS).
i. Applicable to MIIs: MIIs shall conduct self-assessment of their cyber resilience using Cyber Capability Index (CCI) on a quarterly basis.

iii. **DETECT**

a. REs shall establish appropriate security mechanism through Security Operation Centre (SOC) [RE's own SOC, third-party SOC, or a managed SOC] for continuous monitoring of security events and timely detection of anomalous activities.
b. Functional efficacy of SOC shall be measured on a half-yearly basis. A quantifiable method and indicative (but not limited to) list of parameters for measuring SOC efficacy has been formulated.
c. Applicable to MIIs: MIIs shall conduct red teaming exercise as part of their cybersecurity framework.

iv. **RESPOND**

a. All REs shall formulate an up-to-date Cyber Crisis Management Plan (CCMP).
b. Comprehensive Incident Response management plan and respective SOPs shall be established by REs.
c. Alerts generated from monitoring and detection systems shall be suitably investigated for Root Cause Analysis (RCA).

v. **RECOVER**

a. A comprehensive response and recovery plan shall be documented and get triggered for the timely restoration of systems affected by the cyber incident.
b. An indicative (but not limited to) recovery plan has been attached.
c. Actions taken during recovery process shall be informed to all related stakeholders.

The framework will continue to be updated and improved as technology and securities market evolves as different REs provide their feedback. This will ensure that the framework is meeting the cybersecurity needs of securities market, MIIs and all other REs.

Table of Contents

Abbreviations

Sr. No.	Abbreviation	Explanation/Expansion
1.	AIF	Alternative Investment Fund
2.	AMC	Asset Management Company
3.	API	Application Programming Interface
4.	BAS	Breach and Attack Simulation
5.	BYOD	Bring Your Own Device
6.	CART	Continuous Automated Red Teaming
7.	CEO	Chief Executive Officer
8.	CII	Critical Information Infrastructure
9.	CIS	Center for Internet Security
10.	CISO	Chief Information Security Officer
11.	CTI	Cyber Threat Intelligence
12.	DB	Database
13.	DEV	Development
14.	DLP	Data Loss Prevention
15.	DR	Disaster recovery
16.	EDR	Endpoint Detection and Response
17.	EPP	Endpoint Protection Platforms
18.	FDE	Full-disk Encryption
19.	HPSC-CS	High Powered Steering Committee - Cyber Security
20.	GoI	Government of India
21.	IBT	Internet Based Trading
22.	IDS	Intrusion Detection System
23.	IOSCO	International Organization of Securities Commissions

24.	IS	Information Security
25.	ISMS	Information Security Management System
26.	ISO	International Organization for Standardization
27.	IT	Information Technology
28.	MD	Managing Director
29.	MFA	Multi-factor Authentication
30.	MII	Market Infrastructure Institution
31.	MTTC	Mean Time to Contain
32.	MTTD	Mean Time to Detect
33.	MTTR	Mean Time to Resolve
34.	NCIIPC	National Critical Information Infrastructure Protection Centre
35.	NDR	Near Disaster Recovery
36.	NIST	National Institute of Standards and Technology
37.	OS	Operating System
38.	OT	Operational Technology
39.	OWASP	Open Web Application Security Project
40.	PDC	Primary Data Centre
41.	PII	Personal Identifiable Information
42.	PIM	Privileged Identity Management
43.	QA	Quality Assurance
44.	RCA	Root Cause Analysis
45.	RE	Regulated Entity[5]
46.	RPO	Recovery Point Objective
47.	RTO	Recovery Time Objective

[5] Refer Securities Contracts (Regulation) Act 1956, SEBI Act 1992, and Depository Act 1996.

48.	SBOM	Software Bill of Materials
49.	SCOT	Standing Committee on Technology
50.	SOC	Security Operations Centre
51.	SOP	Standard Operating Procedure
52.	SIT	System Integration Test
53.	SSDLC	Secure Software Development Life Cycle
54.	TLP	Traffic Light Protocol
55.	UAT	User Acceptance Test
56.	VAPT	Vulnerability Assessment & Penetration Testing
57.	VBA	Visual Basic for Application
58.	VPN	Virtual Private Network
59.	WAF	Web Application Firewall

Definitions

1. Critical assets –
   Entities shall identify and classify their critical IT systems. Following systems shall be included in critical systems (both on premise and cloud):
   a. Any system that will have adverse impact on any business operations if compromised.
   b. Stores/transmits any type of critical data (financial data, trading data, and PII)
   c. Devices/Network through which any critical system is connected (either physically or virtually).
   d. Internet facing applications / systems
   e. Systems directly/indirectly connected to any other critical system.
   d. All the ancillary systems used for accessing/communicating with critical systems either for operation or for maintenance.

2. Cyber Capability Index (CCI) –
   SEBI has developed a CCI based on the recommendations of HPSC-CS to rate the preparedness and resilience of the cybersecurity framework of the MIIs. CCI is calculated based on 24 parameters extracted from NIST publication *'Performance Measurement Guide for Information Security'*.

3. ISO 27001 certification –
   ISO 27001 certification is a globally recognized standard for Information Security Management Systems (ISMS) published by the International Organization for Standardization (ISO). It helps organizations to become risk-aware, promotes a holistic approach to information security, proactively identify, and address weaknesses.

4. Market Infrastructure Institutions (MII) –
   Stock Exchanges, Depositories and Clearing Corporations are collectively referred to as Market Infrastructure Institutions (MIIs).

5. Principle of Least Privilege (PoLP) –
   Principle of Least Privilege (PoLP) is security concept in which a user or entity shall only have minimum level access to the specific data, resources and applications needed to complete their required task.

6. Red team exercise –
   An exercise, reflecting real-world conditions that is conducted as a simulated adversarial attempt to compromise organizational missions or business processes

and to provide a comprehensive assessment of the security capabilities of an organization and its systems. – Definition from **NIST SP 800-53**[6]

7. Regulated Entity (RE) –
   The term 'Regulated Entity' refers to SEBI registered / recognised intermediaries (for example brokers, mutual funds, KYC Registration Agencies, QRTAs, etc.) and Market Infrastructure Institutions (Stock Exchanges, Depositories and Clearing Corporations) regulated by SEBI.

8. Risk –
   As defined by NIST[7] and OWASP[8], Risk = Likelihood * Impact; where Likelihood = Threat * Vulnerabilities. Likelihood is a measure of how likely a vulnerability is to be discovered and exploited by an attacker. Impact is the magnitude of harm that can be expected as result from the consequences of threat exploitation.

9. Risk-based Authentication (RBA) –
   Risk-based authentication is a non-static authentication mechanism which takes into account the profile of the agent requesting to the system to determine the risk profile associated with that transaction. It checks and applies varying level of stringency to authentication processes based on the likelihood that access to a given system could result in its being compromised.

10. Root Cause Analysis (RCA) –
    The NIST[9] has defined RCA as a principle-based, systems approach for the identification of underlying causes associated with a particular set of risks.

11. Secure Software Development Life Cycle (SSDLC) –
    Secure Software Development Life Cycle (SSDLC) involves integrating security testing at every stage of software development, from design, to development, to deployment and beyond.

12. Specified Regulated Entities (Specified REs) –
    Specified REs are SEBI REs which are critical from the securities market point of view. They are identified on the basis of business volume, market share, business complexity, number of clients, etc. and thus require more stringent cybersecurity measures for the protection of their IT infrastructure than rest of the REs.
    The securities market institutions which fall under the criteria mentioned below will be referred as **Specified REs**.

[6] Refer NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information System and Organizations https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[7] Refer NIST SP 800-30 Rev. 1: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[8] Refer Risk-rating methodology: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

[9] Refer NIST SP 800-30 Rev. 1: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Criteria for Specified REs will be finalized after consultation with market intermediaries/participants, and practitioners.

Table 1: List of Specified REs and their criteria

S. No.	Regulated Entities (REs)	Criteria
1.	**Stock Brokers / Depository Participants**	
2.	**Asset Management Companies (AMCs) / Mutual Funds**	
3.	**KYC Registration Agencies (KRAs)**	
4.	**Qualified Registrars to an Issue / Share Transfer Agents (QRTAs)**	
5.	**Portfolio Managers**	
6.	**Alternative Investment Funds (AIFs)**	

A. Introduction

Technology has become an integral part of securities market since IT industry boomed in India. With these technological developments in securities market, maintaining robust cybersecurity and cyber resilience to protect the organizations operating in securities market from cyber-risks / incidents has become indispensable. SEBI has issued targeted cybersecurity and cyber resilience frameworks for various REs since 2015. To further strengthen cyber-risks / incidents prevention, preparedness, and response capacities, this consolidated cybersecurity and cyber resilience framework has been released.

The consolidated CSCRF will supersede following SEBI circulars which will get deprecated from ***<DD/MM/YYYY>***:

Table 2: List of SEBI cybersecurity circulars to get supersede with CSCRF

S. No.	**Regulated Entity**	**Circular Subject (Circular Number)**	**Date of issuance**
1.	MIIs	Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporation and Depositories (CIR/MRD/DP/13/2015)	July 06, 2015
		Modification in Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporations and Depositories (SEBI/HO/MRD1/MRD1_DTCS/P/CIR/2022/68)	May 20, 2022
2.	Stock Brokers / Depository Participants	Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants (SEBI/HO/MIRSD/CIR/PB/2018/147)	December 03, 2018
		Modification in Cyber Security and Cyber resilience framework for Stock Brokers / Depository Participants (SEBI/HO/MIRSD/TPD/P/CIR/2022/80)	June 07, 2022
		Modification in Cyber Security and Cyber resilience framework for Stock Brokers / Depository Participants (SEBI/HO/MIRSD/TPD/P/CIR/2022/93)	June 30, 2022
3.	Mutual Funds /	Cyber Security and Cyber Resilience framework for Mutual Funds / Asset	January 10, 2019

	Asset Management Companies (AMCs)	Management Companies (AMCs) (SEBI/HO/IMD/DF2/CIR/P/2019/12)	
		Modification in Cyber Security and Cyber Resilience Framework of Mutual Funds/ Asset Management Companies (AMCs) (SEBI/HO/IMD/IMD-I/DOF2/P/CIR/2022/81)	June 09, 2022
4.	KYC Registration Agencies (KRAs)	Cyber Security &Cyber Resilience framework for KYC Registration Agencies (SEBI/HO/MIRSD/DOP/CIR/P/2019/111)	October 15, 2019
		Modification in Cyber Security and Cyber resilience framework of KYC Registration Agencies(KRAs) (SEBI/HO/MIRSD/DoP/P/CIR/2022/74)	May 30, 2022
		Modification in Cyber Security and Cyber resilience framework of KYC Registration Agencies (KRAs) (SEBI/HO/MIRSD/TPD/P/CIR/2022/95)	July 05, 2022
5.	Qualified Registrars to an Issue / Share Transfer Agents (QRTAs)	Cyber Security and Cyber Resilience framework for Registrars to an Issue/ Share Transfer Agents (hereinafter referred to as RTAs) (SEBI/HO/MIRSD/CIR/P/2017/100)	September 08, 2017
		Cyber Security & Cyber Resilience framework for Qualified Registrars to an Issue / Share Transfer Agents (SEBI/HO/MIRSD/DOP/CIR/P/2019/110)	October 15, 2019
		Modification in Cyber Security and Cyber resilience framework of Qualified Registrars to an Issue and Share Transfer Agents(“QRTAs”) (SEBI/HO/MIRSD/MIRSD_RTAMB/P/CIR/2022/73)	May 27, 2022
		Modification in Cyber Security and Cyber resilience framework of Qualified Registrars to an Issue and Share Transfer Agents (“QRTAs”) (SEBI/HO/MIRSD/TPD/P/CIR/2022/96)	July 06, 2022

6	Portfolio Managers	Cyber Security and Cyber Resilience framework for Portfolio Managers (SEBI/HO/IMD/IMD-PoD-1/P/CIR/2023/046)	March 29, 2023

B. Framework Compliance, Audit, Report submission, and Timeline:

This section provides details regarding submission of compliance to this master framework, ISO audit, VAPT, Cyber audit, and timelines for these audits and compliance.

1. ISO Audit and Certification

1.1. Evidence of ISO certifications shall be submitted as follows:

Table 3: REs and their corresponding entity for ISO certification evidence submission

Sr. No.	Regulated Entity	ISO certification and report submission to
1.	Stock Brokers / Depository Participants	Stock exchanges/Depositories
2.	MIIs and rest of the REs	SEBI

2. VAPT[10]

The VAPT scope, periodicity and compliance is defined in the clause D.3.1.3.a. ii.

2.1. The VAPT reporting format has been attached as **Annexure-A**. The VAPT activity report of SEBI REs, required declaration from MD/ CEO to certify compliance and the audit materiality metrics as given in **Annexure-B** shall be submitted as per below table:

Table 4: REs and their corresponding entity for VAPT report submission

Sr. No.	Regulated Entity	VAPT report submission to
1.	Stock Brokers / Depository Participants	Stock exchanges / Depositories
2.	MIIs and rest of the REs	SEBI

2.2. The Periodicity of the VAPT activity for SEBI REs in a financial year shall be as follows:

[10] Unless otherwise specified, all certifications / audits mentioned in consolidated CSCRF have to be conducted by CERT-In empanelled auditor.

Table 5: VAPT periodicity of REs

Sr. No.	Regulated Entity	Periodicity
1.	REs which have been identified as ‘Protected system’ and/or CII by NCIIPC	At least twice In every half of the financial year, one VAPT activity shall get completed (includes report submission, closure, revalidation)
2.	Rest of the REs	At least once VAPT activity shall get started in first quarter of the financial year.

2.3. The timeline for completion of VAPT activity for SEBI REs shall be as follows:

Table 6: Timeline of VAPT report submission and closure compliance for REs

Sr. No.	Activity	Timeline
1.	Final report submission to required authority	Within 1 month of completion of VAPT activity and taking approval from respective technology committees
2.	Compliance of closure of finding identified during VAPT activity	Within next 3 months A graded approach (based on the criticality of observation in terms of impact) shall be followed for closure of the observations found during VAPT.
3.	Revalidation / Audit of VAPT	Within next 1 month

3. Cyber Audit

Cyber audit[11] here pertains to the audit for the compliance with this framework.

3.1. The periodicity of the cyber audit for SEBI REs in a financial year shall be as follows:

Table 7: Cyber audit periodicity of REs

Sr. No.	Regulated Entity	Periodicity
1.	MIIs and Specified REs	At least twice
2.	Rest of the REs	At least once

3.2. The timeline of the cyber audit for SEBI REs shall be as follows:

Table 8: Timeline of Cyber audit findings closure and compliance for REs

Sr. No.	Activity	Timeline
1.	Compliance of closure of finding identified during cyber audit	Within next 3 months A graded approach (based on the criticality of observation in terms of impact) shall be followed for closure of the observations found during VAPT.

3.3. A submission for compliance to this consolidated CSCRF shall be done by all REs. The format for compliance submission to this consolidated CSCRF has been attached as **Annexure-C**. The cyber audit reports for compliance to this consolidated CSCRF, required declaration from MD/ CEO to certify compliance and the audit materiality metrics as given in **Annexure-B** shall be submitted as per below table:

Table 9: REs and their corresponding entity for cyber audit report submission

Sr. No.	Regulated Entity	Cyber audit and declaration report submission to

[11] Unless otherwise specified, all certifications / audits mentioned in consolidated CSCRF have to be conducted by CERT-In empanelled auditor.

1.	Stock Brokers / Depository Participants	Stock exchanges / Depositories
2.	MIIs and rest of the REs	SEBI

4. Periodicity of other Standards/Guidelines

Periodicity of other standards/guidelines mentioned in this consolidated CSCRF shall be as follows:

Table 10: Periodicity of other standards mentioned in CSCRF

Sr. No.	Standard/Guidelines and Clause	Periodicity
1.	Self-assessment of REs' cyber resilience using CCI (1.2.2.b)	Quarterly
2.	Submission of self-assessment evidence using CCI by RE (1.2.3.b.ii.1)	Within first 15 days of next quarter
3.	RE's cybersecurity and cyber resilience policy review (1.2.2.c)	Annually
4.	Internal Technology Committee – For rest of the REs (1.2.3.a.ix)	Quarterly
5.	Standing Committee on Technology – For MIIs (1.2.3.b.i)	Quarterly
6.	Cybersecurity scenario-based drill exercise for risk management (1.3.2.b)	Quarterly
7.	REs' risk assessment (1.3.2.c)	Half-yearly
8.	User access rights review (2.1.2.c)	Quarterly
9.	Review of ex-employee passwords not being used across multiple accounts (2.1.3.a.i.8)	Quarterly
10.	Review of privileged users' activities (2.1.3.c.ii.3)	Quarterly
11.	Cybersecurity training program (2.2.2.c)	Annually

12.	Review of RE’s systems managed by 3rd-party service providers (2.4.3.a.iv.1)	Half-yearly
13.	Red Teaming exercise for MIIs and Specified REs (3.2.2.a)	Half-yearly
14.	Drills for testing adequacy and effectiveness of recovery plan (5.1.2.c)	Quarterly

C. Cybersecurity Framework

1. The framework is based on five concurrent and continuous functions of cybersecurity as defined by NIST[12] – Identify, Protect, Detect, Respond, and Recover.
   a. **IDENTIFY**
   The Identify function assists in developing an organizational understanding of managing cybersecurity risk to systems, people, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.
   b. **PROTECT**
   The Protect function outlines appropriate safeguards to ensure delivery of critical infrastructure services. The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event.
   c. **DETECT**
   The Detect function defines the appropriate activities to identify the occurrence of a cybersecurity event. The Detect function enables timely discovery of cybersecurity events.
   d. **RESPOND**
   The Respond function includes appropriate activities to take action regarding a detected cybersecurity incident. The Respond function supports the ability to contain the impact of a potential cybersecurity incident.
   e. **RECOVER**
   The Recover function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover function supports timely recovery to normal operations and reduce the impact from a cybersecurity incident.

2. Each function covers different security controls. The controls are divided into three categories namely objectives, standards, and guidelines:
   a. **Part-1: Objective**
   The objective highlights the goals which a specific security control wants to achieve.
   b. **Part-2: Standard**
   The standard represents established principles for the cybersecurity framework compliance.
   c. **Part-3: Guidelines**

[12] Cybersecurity Framework's five functions defined by NIST: https://www.nist.gov/cyberframework/online-learning/five-functions

The guidelines are divided into three parts:

i. Applicable to all REs: Baseline cybersecurity measures which will be mandatory and applicable to all REs.

ii. Applicable to Specified REs: Additional cybersecurity measures and guidelines, which are supplementary in nature and will be applicable to **specified REs** as defined.

iii. Applicable to MIIs: Additional cybersecurity guidelines applicable to MIIs.

D. Cybersecurity Framework Functions

1. IDENTIFY

1.1. ID.AM: Asset Management

The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistently with their relative importance to organizational objectives and the organization's risk strategy.

1.1.1. ID.AM: Objective:

a. Physical devices and systems within the organization are inventoried.

b. Software platforms and applications within the organization are inventoried.

c. Organizational communication and data flows are mapped.

d. External information systems are catalogued.

e. Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.

f. Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, and partners) are established.

1.1.2. ID.AM: Standard:

a. An up-to-date inventory shall be maintained by the organization covering (including but not limited to) all hardware, software, cloud assets, API endpoints and information assets. Any changes in the asset inventory shall be reflected within 24 hours.

b. Identification of vulnerabilities, cyber threats with their likelihood shall be identified.

c. Board / Partner / Proprietor shall approve the list of critical systems.

d. Third-party service providers and outsourcing staff shall also be mandated to follow similar standards of information security.

1.1.3. ID.AM: Guidelines:

a. Applicable to all REs:

i. All REs shall identify and classify critical assets based on their sensitivity and criticality for business operations, services and data management. The Board/Partners/Proprietors of the REs shall approve the list of critical systems.

ii. All REs shall maintain up-to-date inventory of its (including but not limited to) hardware and systems, software, cloud assets, API endpoints and information assets (internal and external), details of its network resources, connections to its network and data flows.

iii. Any additions/deletions or changes in existing assets shall be reflected in the asset inventory within 24 hours.

iv. For conducting criticality assessment of assets, REs shall maintain comprehensive asset inventory, conduct threat modelling, vulnerability assessment, etc.

v. REs shall prepare and maintain an up-to-date network architecture diagram at the organisational level including wired/wireless networks.

vi. All REs shall also encourage its third-party service providers to have similar standards of Information Security.

b. Applicable to specified REs and MIIs

i. **Specified REs and MIIs** shall accordingly identify cyber risks[13] that they may face, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.

1.2. ID.GV: Governance

The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and cybersecurity risks are informed to the management.

1.2.1. ID.GV: Objective:

a. Organizational cybersecurity policy is established and communicated.

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

c. Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.

d. Cybersecurity risks are addressed through governance and risk management processes.

1.2.2. ID.GV: Standard:

a. A comprehensive cybersecurity and cyber resilience policy shall be documented and implemented with approval from Board /

[13] Refer Definitions section for the Risk definition.

Partners / Proprietors. The cybersecurity and cyber resilience policy may include guidelines mentioned in this consolidated CSCRF.

b. Clear definition of ownership, custodian of every asset and a proper approval command chain process shall be established and followed.

c. The cyber-security and cyber resilience policy shall be reviewed periodically[14].

d. MIIs shall self-assess their cyber resilience using CCI on a periodic[15] basis.

1.2.3. ID.GV: Guidelines:

a. Applicable to all REs

i. As part of the operational risk management framework to manage risk to systems, networks and databases from cyber-attacks and threats, **REs** shall formulate a comprehensive Cybersecurity and Cyber Resilience policy document encompassing the framework mentioned hereunder. In case of deviations from the suggested framework, reasons for such deviations, technical or otherwise, shall be provided in the policy document.

The policy document shall be approved by the Board / Partners / Proprietors of the **REs**. The policy document shall be reviewed by the aforementioned group periodically with the view to strengthen and improve its Cybersecurity and Cyber Resilience framework.

ii. The cybersecurity policy shall include (but not limited to) policy with respect to asset management, patch management, vulnerability management, audit policy, VAPT policy, monitoring of the network and endpoints, configuration management, change management, software development life cycle management, authentication policies, authorization policies and processes, network segmentation policies, commissioning internet facing assets, encryption policies, PII and privacy policies, cybersecurity control management policy, asset ownership documentation, and chain of command for any approval process in the organization with respect to cybersecurity. It shall also contain do's and don'ts allowed in the organization with respect to usage of cyber

[14] Refer Table 10 in 'Framework Compliance, Audit, Report submission, and Timeline' section.

[15] Refer Table 10 in 'Framework Compliance, Audit, Report submission, and Timeline' section.

assets including desktops, laptops, BYOD, network, internet, etc.

iii. The Cybersecurity Policy shall include the following process to identify, assess, and manage Cybersecurity risk associated with processes, information, networks and systems:

a. ‘Identify’ critical IT assets and risks associated with such assets.

b. ‘Protect’ assets by deploying suitable controls, tools and measures.

c. ‘Detect’ incidents, anomalies and attacks through appropriate monitoring tools/processes.

d. Respond’ by taking immediate steps after identification of the incident, anomaly or attack.

e. ‘Recover’ from incident through incident management and other appropriate recovery mechanisms.

iv. **REs** shall designate a senior official or management personnel (henceforth, referred to as the “Designated Officer”) whose function would be to assess, identify, and reduce cybersecurity risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the cybersecurity Policy.

v. **REs** shall establish a reporting procedure to facilitate communication of unusual activities and events to the Designated Officer in a timely manner.

vi. **REs** shall define responsibilities of its employees, outsourced staff, and employees of third-party service providers, members or participants and other entities, who may have privileged access or use their systems / networks towards ensuring the goal of cybersecurity.

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

viii. As part of compliance management with respect to this consolidated CSCRF, REs shall apply following key aspects (including but not limited to) for implementing compliance management:

1. Assess Compliance with applicable laws, regulations, circulars etc.
2. Develop compliance policies and procedures
3. Implement controls such as security measures
4. Train employees
5. Monitor and review compliance management process
6. Regular audits and reporting.

ix. The Board / Partners / Proprietor of the REs shall constitute an internal Technology Committee comprising experts proficient in Technology. This Technology Committee of **REs** shall meet on a periodic[16] basis to review the implementation of the cybersecurity and cyber resilience policy approved by their Board, and such review shall include goal setting for a target level of cyber resilience, and establish a plan to improve and strengthen cybersecurity and cyber resilience. The review shall be placed before the Board of REs for appropriate action.

b. Applicable to MIIs

i. The Oversight Standing Committee on Technology[17] of the stock exchanges and of the clearing corporations and the IT Strategy Committee[18] of the depositories shall on a periodic[19] basis review the implementation of the cybersecurity and resilience policy approved by their Boards, and such review shall include review of their current IT and cybersecurity and resilience capabilities, set goals for a target level of cyber resilience, and establish a plan to improve and strengthen cybersecurity and cyber resilience.

ii. Cyber Capability Index (CCI)

1. MIIs shall conduct self-assessment of their cyber resilience using CCI and submit corresponding evidences on a periodic[20] basis. A reference of CCI and its calculation methodology has been attached as **Annexure-J**.
2. The indicators used in CCI and their weightage will be reviewed on a half-yearly basis to keep it updated and relevant.

c. Applicable to specified REs and MIIs

i. The cybersecurity policy shall encompass the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC)

[16] Refer Table 10 in ‘Framework Compliance, Audit, Report submission, and Timeline’ section.

[17] Refer SEBI Circulars SMD/POLICY/Cir-2/98 dated January 14, 1998 and CIR/MRD/DSA/33/2012 dated December 13, 2012.

[18] Refer SEBI CIR/MRD/DMS/ 03 /2014 dated January 21, 2014.

[19] Refer Table 10 in ‘Framework Compliance, Audit, Report submission, and Timeline’ section.

[20] Refer Table 10 in ‘Framework Compliance, Audit, Report submission, and Timeline’ section.

of National Technical Research Organisation (NTRO), Government of India in the report titled ‘Guidelines for Protection of National Critical Information Infrastructure’ and subsequent revisions, if any, from time to time.

ii. Specified REs and MIIs shall appoint a senior cybersecurity expert as CISO who will work as a ‘Designated officer’.

iii. **Specified REs and MIIs** shall also incorporate best practices from standards such as ISO 27001, ISO 27002, COBIT 5, etc. or their subsequent revisions, if any, from time to time. ISO 27001 is recommended to be taken as the base standard for governance and management of information security policies.

iv. The aforementioned committee and the senior management of the REs and MIIs, including the CISO, shall periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen cybersecurity and cyber resilience framework.

1.3. ID.RARM: Risk Assessment and Risk Management Strategy

The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

1.3.1. ID.RARM: Objective:

a. Asset vulnerabilities are identified and documented.

b. Cyber threat intelligence is received from information forums and sources.

c. Threats, both internal and external, are identified and documented.

d. Potential business impacts and likelihoods are identified.

e. Threats, vulnerabilities, likelihoods, impacts are used to determine risk.

f. Risk responses are identified and prioritized.

g. Risk management processes are established, managed, and agreed to by organizational stakeholders.

h. Organizational risk tolerance is determined and clearly expressed.

i. The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.

1.3.2. ID.RARM: Standard:

a. Risk factor shall be assessed and managed for all IT assets of the organization.

b. Different scenarios and their respective responses shall be documented and tested on a periodic[21] basis to check the risk management plan of the organization.

c. Risk assessment of organization’s IT environment shall be done on a periodic[22] basis.

1.3.3. ID.RARM: Guidelines:

a. Applicable to all REs

i. Risk assessment

1. All REs shall conduct a risk assessment of the IT environment of their organization on a half-yearly basis to acquire visibility and a reasonably accurate assessment of the overall cybersecurity risk posture. Risk assessment shall result into quantified cybersecurity risk of the RE.

ii. Risk Management

1. REs shall consider using ISO/IEC 27005:2022 or its subsequent revision, from time to time, as the base document for obtaining guidance on information security risk management.
2. Risk management strategy of REs shall include (but not limited to) steps for risk assessment, risk analysis, risk mitigation, risk monitoring and review, compliance with relevant laws and regulations, communication of risk management policies to all stakeholders, effective mitigating measures with options for compensatory controls where feasible, reduced residual risk and ensuring that the cybersecurity risk tolerance is within acceptable limits.
3. REs shall use metrics like (including but not limited to) MTTD, MTTR, MTTC, number of security incidents detected and resolved within a specific period, number of false positives and false negatives generated by security monitoring tools, and how these numbers are being reduced through continuous refinement of the monitoring process, number of security incidents detected and resolved within a specific period, level of employee security awareness, phishing test success rate, how many devices on the network are running end-of-life (EOL) software no longer receiving security

[21] Refer Table 10 in ‘Framework Compliance, Audit, Report submission, and Timeline’ section.

[22] Refer Table 10 in ‘Framework Compliance, Audit, Report submission, and Timeline’ section.

updates, unidentified devices on the internal network, integration of third-party devices and services into the network and process for managing their access and permissions, patching cadence, security rating, third-party security rating, number of known vulnerabilities, number of intrusion attempts detected and blocked by the IDS, number of successful cyber-attacks occurred in the past year, etc. to assess cybersecurity posture of their organization.

4. Adequate manpower in cybersecurity domain shall be hired to safeguard organization from any cyber risk / threat / incident.

iii. Risk-based authentication (RBA)

1. Risk assessment of Authentication-based server shall be done to get insights about context behind every login to servers.
2. When a user attempts to sign-in, risk-based authentication solution shall analyse factors such as device, location, network, sensitivity, etc.

iv. Cyber Threat Intelligence (CTI)

1. REs shall harness CTI provided by CISO forum or CERT-In or any third-party vendor to transform security decision-making when addressing attacks by threat actors, making it more informed, quicker and data driven.

v. Cybersecurity scenario-based Testing

1. Comprehensive scenario-based testing shall be done for assessing risk related to cybersecurity in the organization’s IT assets.
2. Possible attack scenarios and possibilities have been attached as **Annexure-D**.

1.4. ID.SC: Supply Chain Risk Management

The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risks. The organization has established and implemented the processes to identify, assess and manage supply chain risks.

1.4.1. ID.SC: Objective:

a. Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.

b. Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber-supply chain risk assessment process.

c. Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and cyber-supply chain risk management plan.

d. Suppliers and third-party partners are routinely assessed using audits, test results, and/or other forms of evaluations to confirm that they are meeting their contractual obligations.

e. Response and recovery planning and testing are conducted along with suppliers and third-party providers.

1.4.2. ID.SC: Standard:

a. Concentration risk on outsourced agencies shall be assessed and reviewed.

b. Manpower adequacy in cybersecurity domain shall be estimated and monitored.

1.4.3. ID.SC: Guidelines:

a. Applicable to all REs

i. <u>Concentration risk on third-party service providers / outsourced agencies</u>

1. REs need to take into account concentration risk while outsourcing multiple critical services to the same third-party service provider.
2. It has also been observed that single third-party service providers are providing services to multiple REs, which creates concentration risk. Here, such third parties though being small non-financial organizations, if any cyber-attack happens at such organizations, the same could have systemic implication due to high concentration risk. SEBI circular on '*Guidelines on Outsourcing of Activities by Intermediaries*'[23] has been attached as **Annexure-E** and shall be complied by all REs.
3. REs shall prescribe specific cybersecurity controls, including audit of their systems and protocols from independent auditors, to mitigate such concentration risk.

ii. <u>Software Bill of Materials (SBOMs)</u>

1. REs shall obtain SBOMs for any new products before they procure it. SBOMs containing all the open source and third-

[23] Refer SEBI CIR/MIRSD/24/2011 dated December 15, 2011.

party components present in a codebase, versions of the components used in the codebase, and their patch status allows security teams to quickly identify any associated security or license risks.

2. SBOM shall include license information, name of the supplier, all primary (top level) components with all their transitive dependencies (include third-party dependencies whether an in-house or open-source component) and relationships, cryptographic hash of the components, frequency of updates, known unknown (where a SBOM does not include a full dependency graph) access control and methods for accommodating occasional incidental errors.

iii. Manpower deployment

1. Based on the risk assessment, hiring and deployment of professionals/experts in cybersecurity domain on full-time/part-time/contract basis shall be made to ensure cyber resiliency of the REs.
2. Adequate manpower in cybersecurity domain shall be hired to safeguard organization from any cyber risk / threat / incident.

2. PROTECT

2.1. PR.AC: Identity Management, Authentication, and Access Control

Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed in consistent with the assessed risk of unauthorized access to authorized activities and transactions.

2.1.1. PR.AC: Objective:

a. Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.

b. Physical access to assets is managed and protected.

c. Remote access is managed.

d. Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.

e. Network integrity is protected (e.g., network segregation, network segmentation).

f. Identities are proofed and bound to credentials and asserted in interactions.

g. Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).

2.1.2. PR.AC: Standard:

a. While giving access to both on premise and cloud resources of the organization, 'Principle of Least Privilege' and 'Zero Trust Model' shall be followed. PIM solutions shall be mandated for keeping track of privileged access.
b. Critical systems shall have MFA implemented for all users.
c. Access rights shall be reviewed on a periodic[24] basis.
d. User logs shall be uniquely identified and stored for at least 2 years.
e. A comprehensive password policy shall be documented and implemented.
f. Physical access to the critical systems shall be monitored and recorded on a daily basis.
g. Access restriction shall be there for outsourced staff. If access grant is required in special case, it shall be for the limited time-period and shall be subject to stringent supervision and monitoring.
h. Strong authentication and authorization mechanisms shall be enforced for API security.
i. A comprehensive Data-disposal and data-retention policy shall be documented and implemented.
j. Proper SOPs shall be documented for handling storage media devices and their disposal.

2.1.3. PR.AC: Guidelines

a. Applicable to all REs

i. Access Controls, Password Policy / Authentication Mechanism

1. No person by virtue of rank or position shall have any intrinsic right to access confidential data applications, system resources or facilities.
2. Any access to REs systems, applications, networks, database, etc., shall be for a defined purpose and for a defined period. Access grant to IT systems, applications, databases and networks shall be on a need-to-use basis and based on the principle of least privilege. Such

[24] Refer Table 10 in 'Framework Compliance, Audit, Report submission, and Timeline' section.

access shall be for the period during which the access is required and shall be authorized using strong authentication mechanisms.

3. All critical systems accessible over the internet shall have two-factor security (such as VPNs, Firewall controls, etc.).
4. All REs shall ensure that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes. Such logs shall be maintained and stored in a secure location for a time period not less than two (2) years.
5. Account access lock policies after failure attempts shall be implemented for all accounts.
6. Existing user accounts and access rights shall be periodically reviewed by the owner of the system in order to detect dormant accounts and accounts with excessive privileges, unknown accounts or any type of discrepancy.
7. Proper 'end of life' mechanism shall be adopted for user management to deactivate access privileges of users who are leaving the organization of whose access privileges have been withdrawn. This includes named user IDs and generic user IDs.
8. Strong password policy shall be implemented. The policy shall include a clause for periodic[25] review of accounts of ex-employees passwords shall not be reused across multiple accounts or list of passwords shall not be stored on the system.
9. MFA shall be enabled for all users that connect using online/internet facility and also particularly for virtual private networks, webmail, and accounts that access critical systems.

ii. Log Management

1. An indicative (but not limited to) list of types of log data to be collected by REs are: System logs, Application logs, Network logs, Security logs, and PowerShell logs. REs are advised to ensure that all logs are being collected.
2. Strong log retention policy shall be implemented as per extant SEBI regulations and required by CERT-In and IT Act 2000. Monitoring of all logs of events and

[25] Refer Table 10 in 'Framework Compliance, Audit, Report submission, and Timeline' section.

incidents to identify unusual patterns and behaviours shall be done.

iii. Physical Security

1. Physical access to the critical systems shall be restricted to minimum and only to authorized officials. Physical access provided to outsourced staff/visitors shall be properly supervised by ensuring at the minimum that outsourced staff/visitors are accompanied at all times by authorized employees.
2. Physical access to the critical systems shall be revoked immediately if the same is no longer required.
3. All REs shall ensure that the perimeter of the critical equipment's room, if any, are physically secured and monitored by employing physical, human and procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. wherever appropriate.

iv. Remote Support Service Security

1. As many OEMs and their service partners as well as System Integrators provide remote support services to organisations, REs shall ensure that these services are well-governed, controlled, logged and an oversight maintained on all the activities done by remote support service providers. It shall be complemented by regular inspection and audit to validate the defined policies for privileged remote users and access.

v. Network Security Management

1. REs shall apply appropriate network segmentation techniques to restrict access to the sensitive information, hosts and services. Segment to segment access shall be based on strong access control policy and Principle of Least Privilege.
2. All REs shall install network security devices, such as WAF, proxy servers, IDS to protect their IT infrastructure which is exposed to the internet, from security exposures originating from internal and external sources.
3. Adequate controls shall be deployed to address virus / malware / ransomware attacks on servers and other computer systems. These controls may include host / network / application based IDS systems, customized kernels for Linux, anti-virus and anti-malware software

etc. Updation of anti-virus definition files and automatic anti-virus scanning shall be done on a regular basis.

4. All REs shall establish baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within the IT environment. The LAN and wireless networks shall be secured within their premises with proper access controls. The REs shall conduct regular enforcement checks to ensure that baseline standards are applied uniformly.

vi. Disposal of data, systems, and storage devices

1. REs shall formulate a data-disposal and data-retention policy to identify the value and lifetime of various parcels of data.
2. REs shall frame suitable policy for disposal of storage media and systems. The critical data / information on such devices and systems shall be removed by using methods such as crypto shredding / wiping / cleaning / overwrite / degauss / physical destruction as applicable.

b. Applicable to Stock Brokers / Depository Participants

i. Network Security Management

1. For algorithmic trading facilities, adequate measures shall be taken to isolate and secure the perimeter and connectivity to the servers running algorithmic trading applications.

c. Applicable to specified REs and MIIs

ii. Access Controls, Password Policy / Authentication Mechanism

1. **Specified REs and MIIs** shall implement an access policy which addresses strong password controls for users' access to systems, applications, networks and databases. Illustrative examples for this are given in **Annexure-F**.
2. **Specified REs and MIIs** shall implement strong password controls for users' access to systems, applications, networks and databases. Password controls shall include a change of password upon first log-in, minimum password length and history, password complexity as well as maximum validity period. The user credential data shall be stored using strong and latest hashing algorithms.

3. **Specified REs and MIIs** shall deploy controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users). Such controls and measures shall inter-alia include restricting the number of privileged users, periodic[26] review of privileged users' activities, disallow privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.
4. Employees and outsourced staff such as employees of third-party service providers, who may be given authorized access to the critical systems, networks and other computer resources of **specified REs and MIIs** shall be subject to stringent supervision, monitoring and access restrictions.
5. **Specified REs and MIIs** shall formulate an Internet access policy to monitor and regulate the use of internet and internet based services such as social media sites, cloud-based internet storage sites, etc. within the critical IT infrastructure of **specified REs and MIIs**.

2.2. PR.AT: Awareness and Training

The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity related duties and responsibilities consistent with related policies, procedures, and agreements.

2.2.1. PR.AT: Objective:

a. All users are informed and trained.
b. Privileged users understand their roles and responsibilities.
c. Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.
d. Senior executives understand their roles and responsibilities.
e. Physical and cybersecurity personnel understand their roles and responsibilities.

2.2.2. PR.AT: Standard:

a. A program for building cybersecurity and system hygiene awareness of staff shall be established.
b. A program on cybersecurity and system hygiene shall be made for senior management.

[26] Refer Table 10 in 'Framework Compliance, Audit, Report submission, and Timeline' section.

c. A mandatory training program shall be conducted on a periodic[27] basis to enhance the knowledge and understanding of cybersecurity among the staff.
d. Training programs and programs for system hygiene shall be updated as per the state-of-the-art technologies and industry trends.

2.2.3. PR.AT: Guidelines:

a. Applicable to specified REs and MIIs

i. **Specified REs and MIIs** shall work on building cybersecurity and basic system hygiene awareness of staff (with a focus on staff from non-technical disciplines).

ii. **Specified REs and MIIs** shall conduct periodic training programs to enhance knowledge of IT / cybersecurity Policy and standards among the employees incorporating up-to-date cybersecurity threat alerts. Wherever possible, this shall be extended to outsourced staff, third-party service providers, etc.

iii. The training programs shall be reviewed and updated to ensure that the contents of the program remain current and relevant.

2.3. PR.DS: Data Security

Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.

2.3.1. PR.DS: Objective:

a. Data-at-rest and Data-in-transit is protected.
b. Assets are formally managed throughout removal, transfers, and disposition.
c. Adequate capacity to ensure availability is maintained.
d. Protections against data leaks are implemented.
e. Integrity checking mechanisms are used to verify software, firmware, and information integrity.
f. The development and testing environment(s) are separate from the production environment.
g. Integrity checking mechanisms are used to verify hardware integrity.

[27] Refer Table 10 in ‘Framework Compliance, Audit, Report submission, and Timeline’ section.

2.3.2. PR.DS: Standard:

a. Strong data protection measures (both at-rest and in-transit) with industry standard encryption algorithms shall be put in place.

b. Backup and recovery plan of data shall be documented to ensure that there is no data loss.

c. Appropriate tools shall be put in place to prevent any data leakage.

d. Off-the-shelf products shall be certified with common criteria certification provided by GoI before deploying to production.

2.3.3. PR.DS: Guidelines:

a. Applicable to all REs

i. Data and Storage Devices security

1. Critical data shall be identified and encrypted in motion and at rest by using strong encryption methods. Layering of Full-disk Encryption (FDE) along with File-based Encryption (FBE) shall be used wherever possible. Use industry standard, strong encryption algorithms (eg: RSA, AES, etc.) wherever encryption is implemented. Illustrative measures in this regard are given in **Annexure-G** and **Annexure-H**.
2. Enforce effective data protection, backup, recovery measures.
3. Deploy Data Loss Prevention (DLP) solutions / processes.
4. REs shall block administrative rights on end-user workstations/PCs/laptops and provide access rights on a need-to-know basis and for specific duration for which it is required following an established process and approval.
5. REs shall implement measures to control use of VBA/macros in office documents, control permissible attachment types in email systems.

ii. Application Security in Customer Facing Applications

1. Application security for Customer facing applications offered over the Internet such as IBTs (Internet Based Trading applications), portals containing sensitive or private information and back office applications (repository of financial and personal information offered by **specified REs and MIIs** to Customers) are paramount as they carry significant attack surfaces by virtue of being available publicly over the Internet for

mass use. An illustrative list of measures for ensuring security in such applications is provided in **Annexure-F**.

iii. Certification of off-the-shelf products

1. Stock Exchanges and Depositories shall ensure that vendors empanelled by them for supply of software/product to their respective regulated agencies stock brokers and depository participants shall mandatorily obtain Indian Common Criteria certification of Evaluation Assurance Level 4. **Specified REs and MIIs** shall ensure that off-the-shelf products being used for core business functionality (such as Back office applications) shall bear Indian Common Criteria Certification of Evaluation Assurance Level 4. The Common criteria certification in India is being provided by (STQC) Standardisation Testing and Quality Certification (Ministry of Electronics and Information Technology). In-house software and components need not obtain the certification, but have to undergo intensive regression testing, configuration testing etc. The scope of tests shall include business logic and security controls.

b. Applicable to specified REs and MIIs

i. Data and Storage Devices security

1. **Specified REs and MIIs** 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 confidentiality of information is not compromised during the process of exchanging and transferring information with external parties. Illustrative measures to ensure security during transportation of data over the internet are given in Annexure-H.
2. The information security policy shall also cover use of devices such as mobile phones, photocopiers, scanners, etc., within their critical IT infrastructure, that can be used for capturing and transmission of sensitive data. For instance, defining access policies for personnel, and network connectivity for such devices etc.
3. **Specified REs and MIIs** shall allow only authorized data storage devices within their IT infrastructure through appropriate validation processes.

c. Applicable to MIIs

i. Data and Storage Devices security

1. Along with encrypting data-at-rest and data-in-transit, Confidential Computing shall be used to protect sensitive personal data, sensitive financial data and PII even when it is being processed.

2.4. PR.IP: Information Protection Processes and Procedures

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

2.4.1. PR.IP: Objective:

a. A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality).

b. A System Development Life Cycle to manage systems is implemented.

c. Configuration change control processes are in place.

d. Backups of information are conducted, maintained, and tested.

e. Policy and regulations regarding the physical operating environment for organizational assets are met.

f. Data is destroyed according to policy.

g. Protection processes are continually improved.

h. Effectiveness of protection technologies is shared.

i. Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.

j. Response and recovery plans are tested.

k. IT, OT and IS infrastructure is ‘secure by design’, ‘secure by engineering / implementation’ and the infrastructure has appropriate elements to ensure ‘secure IT operations’.

l. cybersecurity is included in human resources practices (e.g., DE provisioning, personnel screening).

m. A vulnerability management plan is developed and implemented.

2.4.2. PR.IP: Standard:

a. Proper scans of critical software/applications shall be done to ensure no malicious code is present.

b. All anomalies and alerts generated shall be properly investigated and monitored within stipulated time.

c. For all cloud instances of REs, SEBI circular 'Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs)' shall be followed.

d. Recovery Time Objective (RTO) and Recovery Point Objective (RPO) shall be followed with a recovery plan in place for the restoration of systems after cyber-incidents.

e. Only CERT-In empanelled auditors shall be on boarded for external audit of REs.

f. MIIs and Specified REs shall obtain ISO 27001 certification.

g. REs shall follow globally recognised standards like CIS Critical Security Controls to enhance the RE's cyber resilience.

2.4.3. PR.IP: Guidelines:

a. Applicable to all REs

i. Secure Software Development Life Cycle (SSDLC)

1. For the development of all critical software / applications and further feature enhancements, there shall be separate DEV, SIT, UAT, and QA environments.
2. After development of any critical feature enhancement, SIT shall be done to ensure that the complete software / application is working as required.
3. For deployment purpose, rolling updates or Blue-green deployment strategies shall be followed.
4. During the development phase of any software/application to be used by the REs or customers of REs, it shall be ensured that vulnerabilities based on best practices baselines such as OWASP and top 25 software security vulnerabilities identified by CWE/SANS are addressed.
5. All REs shall ensure that regression testing is undertaken before new or modified system is implemented. The scope of test shall cover business logic, security control and system performance under various stress-load scenarios and recovery conditions.
6. For any production release, vulnerability assessment shall be undertaken. For all major release, limited purpose VAPT shall be conducted by the REs to assess the risk and vulnerabilities generated from recent additions in applications / software.
7. For the critical software/applications, undertaking from the OEMs/application providers shall be taken such that application is free from embedded malicious/fraudulent code.

ii. Measures against Phishing attacks / websites

1. The REs need to proactively monitor the cyberspace to identify phishing websites w.r.t. REs domain and report the same to CSIRT-Fin/CERT-In for taking appropriate action.
2. Majority of the infections are primarily introduced via phishing emails, malicious adverts on websites, and third-party apps and programs. Hence, thoughtfully designed security awareness campaigns that stress the avoidance of clicking on links and attachments in email, shall be established as an essential pillar of defence. Additionally, the advisories issues by CERT-In/CSIRT-Fin may be referred for assistance in conducting exercises for public awareness.

iii. Security of Cloud Services

1. Check public accessibility of all cloud instances in use. Make sure that no server/bucket is inadvertently leaking data due to inappropriate configurations.
2. Proper security of cloud access tokens[28] shall be ensured. The tokens shall not be exposed publicly in website source code, any configuration files etc. SEBI circular 'Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs)' has been attached as **Annexure-I** and shall be complied by all REs.

iv. Systems managed by third-party service providers

1. REs have outsourced many of their critical activities to different agencies / vendors / third-party service providers. The responsibility, accountability and ownership of those outsourced activities lies primarily with REs. Therefore, REs have to come out with appropriate monitoring mechanism through clearly defined framework to ensure that all the requirements as specified in this framework is complied with. The periodic[29] report submitted to SEBI shall highlight the critical activities handled by the agencies and to certify the above requirement is complied.
2. Where the systems (IBT, Back office and other Customer facing applications, IT infrastructure, etc.) of a RE are managed by third-party service providers and

[28] Refer SEBI/HO/ITD/ID_VAPT/P/CIR/2023/033 dated March 06, 2023.

[29] Refer Table 10 in 'Framework Compliance, Audit, Report submission, and Timeline' section.

the RE may not be able to implement some of the aforementioned guidelines directly, the RE shall instruct the third-party service provider to adhere to the applicable guidelines in the cybersecurity and Cyber Resilience framework and obtain the necessary cyber audit certifications from them to ensure compliance with the framework standards.

v. Systems managed by MIIs

1. Where applications are offered to customers over the internet by MIIs (Market Infrastructure Institutions), for eg.: NSE's NOW, BSE's BEST etc., the responsibility of ensuring Cyber Resilience on those applications reside with the MIIs and not with the RE who is getting it from MIIs.

vi. Periodic Audit

1. REs shall engage only CERT-In empanelled auditors for their external audits and to audit the implementation of all standards mentioned in this framework.
2. An auditor empanelled by the REs shall be valid for the maximum period of three consecutive years. After the expiry of audit contract, REs shall wait for at least two years as cooling off period to re-empanel that auditor.
3. The periodicity, timeline and report submission for cyber audit by respective authorities has been provided in the '*Framework compliance, Audit, Report submission, Timeline'* section.
4. Along with the cyber audit reports, henceforth, all REs shall submit a declaration from the Managing Director (MD) / Chief Executive Officer (CEO) certifying that:
    a. Comprehensive measures and processes including suitable incentive / disincentive structures, have been put in place for identification / detection and closure of vulnerabilities in the organization's IT systems.
    b. Adequate resources have been hired for staffing their Security Operations Centre (SOC).
    c. There is compliance by the RE with all SEBI circulars and advisories related to cybersecurity.
5. To ensure that all the open vulnerabilities in the IT assets of REs have been fixed and closed, revalidation / audit of VAPT shall also be done within 30 days of compliance of closure VAPT report given by auditor .

6. Audit Management process of the REs shall include (but not limited to) Audit Program / Audit Calendar, Audit Planning, Audit Preparation, Audit Delivery, Audit Evaluation, Audit Reporting, and Audit Follow-up steps. An indicative (but not limited to) list of audit metrics to help analyse materiality has been attached as **Annexure-B**.
7. Due diligence with respect audit process and tools used for such audit shall be undertaken to ensure competence and effectiveness of audits.

b. Applicable to MIIs

i. ISO Certification

1. ISO 27001 certification shall be mandatory for **MIIs** as it provides essential security standards with respect to ISMS. The scope for ISO 27001 certification shall include (but not limited to) PDC site, DR site, NDR site, SOC.

ii. CIS Critical Security Controls

1. MIIs shall follow latest version of CIS Controls which are prioritized set of safeguards and actions for cyber defence and provide specific and actionable ways to mitigate prevalent cyber-attacks.

2.5. PR.MA: Maintenance

Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.

2.5.1. PR.MA: Objective:

a. Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.

b. Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.

2.5.2. PR.MA: Standard:

a. Patches shall be identified and categorized based on their severity. And, critical patches shall be closed by the earliest.

2.5.3. PR.MA: Guidelines:

a. Applicable to all REs

i. Hardening of Hardware and Software

1. REs shall deploy only hardened and vetted hardware / software. During the hardening process, REs shall inter-alia ensure that default username and password are

replaced with non-standard username and strong passwords and all unnecessary services are removed or disabled in software / system.

2. Hardening of OS shall be done to protect servers'/ endpoints' OS and minimize attack surface and exposure to threats.
3. For running services, non-default ports shall be used. Open ports on networks and systems which are not in use or can be potentially used for exploitation of data shall be blocked. Other open ports shall be monitored and appropriate measures shall be taken to secure them.
4. Practice of whitelisting of ports based on business usage at Firewall level shall be implemented rather than blacklisting of certain ports. Traffic on all other ports which have not been whitelisted shall be blocked by default.
5. Restrict execution of "PowerShell" and "wscript" in the enterprise environment, if not required. Ensure installation and use of latest version of PowerShell, with enhanced logging enabled, script block logging and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis.
6. REs shall utilize host based firewall to prevent Remote Procedure Call (RPC) and Server Message Block (SMB) communication among endpoints whenever possible to limit lateral movement as well as other attack activities.

ii. Patch Management

1. REs shall establish and ensure that the patch management procedures include the identification, categorization and prioritization of patches and updates. An implementation timeframe for each category of patches shall be established to apply them in a timely manner.
2. All operating systems and applications shall be updated with the latest patches on a regular basis. As an interim measure for zero-day vulnerabilities and where patches are not available, virtual patching can be considered for protecting systems and networks. These measures hinders cybercriminals from gaining access to any system through vulnerabilities in end-of-support and end-of-life applications and software. Patches shall be sourced only from the authorized sites of the OEM.

3. REs shall perform rigorous testing of security patches and updates, wherever possible, before deployment into the production environment so as to ensure that application of patches do not impact other systems.
4. All patches shall be tested in non-production environment which is identical to production environment.

2.6. PR.PT: Protective Technology and Resilience

Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

2.6.1. PR.PT: Objective:

a. Endpoint devices, user authentication, removable media is protected and its use restricted according to policy.

b. Proper mechanisms are implemented to achieve resilience requirements in normal and adverse situation.

2.6.2. PR.PT: Standard:

a. Restriction for using endpoint devices, network, user authentication, API security, removable media, BYOD, Laptops / mobiles, etc. shall be defined and implemented.

b. API security with proper authentication and authorization mechanisms shall be defined and implemented.

2.6.3. PR.PR: Guidelines:

a. Applicable to all REs

i. <u>API security</u>

1. API security secures vulnerabilities and misconfigurations in the APIs and prevents their misuse. Thus, effective API security strategies shall be used while developing APIs.
2. Rate limiting and throttling shall be used to save APIs from getting overused or abused.
3. Proper access management, authentication and authorization shall be done to ensure that only desired entities have access to the APIs.
4. OWASP documentation for developing APIs shall be followed and OWASP top 10 API security risks shall be mitigated.

ii. <u>Endpoint security</u>

1. EPP and EDR solutions shall be implemented to provide active threat detection, detect attacks on endpoint devices, and to enable immediate response to incidents.

2. IPS shall be used to continuously monitor the organizations' network for malicious activity.

iii. Guidance on usage of Active Directory (AD) servers

1. All REs shall regularly review the Active Directory (AD) to locate and close existing backdoors such as compromised service accounts, which often have administrative privileges and are a potential target of attacks.

iv. Restricted use of removable media and electronic devices

1. Define and implement policy for restriction and secure use of removable media / BYOD including (but not limited to) laptops / mobile devices, servers, etc. and secure erasure of data to ensure that no data is in recoverable form on such media after use.

b. Applicable to Specified REs and MIIs

ii. Guidelines for Application Security and Emerging Technologies

1. Specified REs and MIIs shall prepare SOPs for open source application security and emerging technologies like Generative AI security concerns.

3. DETECT

3.1. DA.CM: Security Continuous Monitoring

The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

3.1.1. DA.CM: Objective:

a. The network and endpoints are monitored to detect potential cybersecurity events.
b. The physical environment is monitored to detect potential cybersecurity events.
c. Personnel activity is monitored to detect potential cybersecurity events.
d. Malicious code is detected.
e. Unauthorized mobile code is detected.
f. External service provider activity is monitored to detect potential cybersecurity events.
g. Monitoring for unauthorized personnel, connections, devices, and software is performed.
h. Vulnerability scans are performed.

3.1.2. DA.CM: Standard:

a. Security Operations Centre (SOC) shall be up and running 24*7*365 to monitor, prevent, detect, investigate, and respond to cyber threats round the clock.

b. Appropriate continuous security monitoring shall be established in SOC for the timely detection of anomalous or malicious activities.

c. Security audit, Vulnerability Assessment and Penetration Testing (VAPT) shall be conducted to detect open security vulnerabilities in IT environment.

d. Capacity utilization shall be monitored for all the critical assets in the organization.

3.1.3. DA.CM: Guidelines:

a. Applicable to all REs

i. Security Continuous Monitoring

1. REs shall establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events / alerts and timely detection of unauthorized or malicious activities, unauthorized changes, unauthorized access and unauthorized copying and transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices exposed to the internet shall also be monitored for anomalies.
2. Suitable alerts shall be generated in the event of detection of unauthorized or abnormal system activities, transmission errors or unusual online transactions.
3. To enhance the security monitoring system, REs are mandated to employ SOC services for their systems. REs may choose any of the following models to use SOC services:

   a. RE's own SOC

   b. Market SOC setup by MIIs

   c. Any other 3rd party managed SOC

ii. Vulnerability Assessment and Penetration Testing (VAPT)

1. The periodicity, timeline for remedial actions, closure and report submission for VAPT activity by respective authorities has been provided in the '*Framework compliance, Audit, Report submission, Timeline'* section.
2. REs shall regularly conduct security audit / Vulnerability Assessment and Penetration Tests (VAPT) in

accordance with this consolidated CSCRF to detect security vulnerabilities in their IT environments. The assets for VAPT include (but not limited to) all ***critical assets***, infrastructure components (like networking systems, security devices, load balancer, servers, databases, applications, systems accessible through WAN, LAN as well as with Public IP's, websites, etc.), and other IT systems pertaining to the activities done by REs in order to detect security vulnerabilities in the IT environment and in-depth evaluation of the security posture of the system through simulations of actual attacks.

3. In addition, REs shall perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system which is a critical system or part of an existing critical system.
4. The REs which have been identified as CII by NCIIPC are mandated to send regular updates / closure status of the vulnerabilities found in their respective protected system to NCIIPC.
5. VAPT shall be comprehensive in nature and provide in-depth evaluation of the security posture of the REs. An indicative (but not exhaustive and limited to) VAPT scope has been attached as **Annexure-K**.
6. Revalidation of VAPT shall also be done to ensure that all the open vulnerabilities in the REs assets have been fixed and closed.

b. Applicable to specified REs and MIIs

i. Security Continuous Monitoring

1. To ensure high resilience, high availability and timely detection of attacks on systems and networks exposed to the internet, **specified REs and MIIs** shall implement suitable mechanisms to monitor capacity utilization of its critical systems and networks that are exposed to the internet.

c. Applicable to specified REs

i. Vulnerability Assessment and Penetration Testing (VAPT)

1. In case of vulnerabilities discovered in off-the-shelf products (used for core business) or applications provided by stock exchange empanelled vendors,

specified REs shall report them to the vendors and the stock exchanges in a timely manner.

d. Applicable to MIIs

i. Security Continuous Monitoring

1. MIIs shall have a cybersecurity Operation Centre (C-SOC) that would be a 24*7*365 set-up manned by dedicated security analysts to identify, respond, recover and protect from cybersecurity incidents[30]. The C-SOC for MIIs shall function in accordance with SEBI circular CIR/MRD/CSC/148/2018 dated December 07, 2018 which has been attached as **Annexure-L**.

3.2. DA.DP: Detection Process

Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.

3.2.1. DA.DP: Objective:

a. Roles and responsibilities for detection are well defined to ensure accountability.
b. Detection activities comply with all applicable requirements.
c. Detection processes are tested.
d. Event detection information is communicated.
e. Detection processes are continuously improved.

3.2.2. DA.DP: Standard:

a. MIIs and Specified REs shall conduct goal-based adversarial simulation red teaming exercise on a periodic[31] basis to identify potential weaknesses with the organization's cyber defence.

3.2.3. DA.DP: Guidelines:

a. Applicable to all REs

i. Functional efficacy of SOC

1. Functional efficacy of SOC of the REs shall be measured. Further, it is suggested to categorize SOC efficacy parameters into three categories (mandatory, desirable, good to have) for auditing SOC efficacy from governance perspective. A quantifiable method and an indicative (but not exhaustive and limited to) list of parameters for measuring SOC efficacy and parameters categorisation is attached as **Annexure-M**.

[30] Refer SEBI circular CIR/MRD/CSC/148/2018 dated December 07, 2018.

[31] Refer Table 10 in 'Framework Compliance, Audit, Report submission, and Timeline' section.

2. REs shall review the functional efficacy of SOC on a half-yearly basis.

b. Applicable to Specified REs and MIIs

i. MIIs and Specified REs shall deploy BAS, decoy and Vulnerability Management solution to enhance their cybersecurity posture.

ii. Red Teaming exercise

1. MIIs and Specified REs shall conduct red teaming exercises as part of their cybersecurity framework on a half-yearly basis. To begin with, a coordinated red team exercise of MIIs can be conducted. CART solution shall be deployed for continuous and automated process of testing the security of the system and achieve greater visibility on attack surfaces.

4. RESPOND

4.1. RS.RP: Response Planning

Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.

4.1.1. RS.PL: Objective:

a. Response plan is executed during or after an incident.

b. Incidents are contained and mitigated. Further, newly identified vulnerabilities are mitigated or documented as accepted risks.

4.1.2. RS.PL: Standard:

a. A comprehensive response plan shall be documented with scenarios based Standard Operating Procedures (SOP). Also, response plan and execution of specific SOP shall be triggered as soon as an incident occurs.

4.1.3. RS.PL: Guidelines

a. Applicable to all REs

i. Cyber Crisis Management Plan (CCMP)

1. All REs shall formulate an up-to-date Cyber Crisis Management Plan (CCMP).
2. CCMP shall be approved from Board of respective REs.

ii. Incident Response Management

1. All REs shall come up with an Incident Response Management Plan.
2. For incident, following SOPs shall be put in place:

For self	Every REs shall have a SOP for cybersecurity incident response and recovery for itself.
REs under MIIs supervision	Every MII shall have a SOP plan for cybersecurity incident response and recovery for REs under their supervision.
Cyber incident response to SEBI	The SOP to be followed for handling and classifying incidents in the securities market has been attached as **Annexure-O**.

iii. The response plan shall define responsibilities and actions to be performed by its employees and support / outsourced staff in the event of cyber-attacks or breach of cybersecurity mechanism.

4.2. RS.CO: Communication

Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).

4.2.1. RS.CO: Objective:

a. Personnel know their roles and order of operations when a response is needed.
b. Incidents are reported consistent with established criteria.
c. Information is shared consistent with response plan.
d. Coordination with stakeholders occurs consistent with response plans.
e. Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.

4.2.2. RS.CO: Standard:

a. Incident reporting shall be done to SEBI and CERT-In as soon as incident occurs. Further, all stakeholders shall coordinate in response to the cyber incident.

4.2.3. RS.CO: Guidelines:

a. Applicable to all REs

i. Cyber Threat Intelligence

1. REs shall share Threat Intelligence data that is collected, processed, and analysed to gain insights into the motives of an attacker, target, attack pattern and behaviour of the threat actor in SEBI CISO forum.

ii. All Cyber-attacks, threats, cyber-incidents and breaches experienced by REs shall be reported to SEBI within 6 hours of noticing / detecting such incidents or being brought to notice about such incidents. This information shall be shared to SEBI through the Incident Report Portal of SEBI. Stock Brokers / Depository Participants shall report the incidents to Stock Exchanges / Depositories also along with SEBI within 6 hours of notice about such incidents.

iii. The incident shall also be reported to Indian Computer Emergency Response team (CERT-In) in accordance with the guidelines / directions issued by CERT-In from time to time. Additionally, the **REs**, whose systems have been identified as “Protected system” by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC. The quarterly reports containing information on cyber-attacks, threats, cyber-incidents and breaches experienced by REs and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities, threats that may be useful for other REs and SEBI, shall be submitted to SEBI within 15 days from the quarter ended June, September, December and March of every year.

iv. Such details as are felt useful for sharing with other REs and MIIs in masked manner shall be shared using mechanism to be specified by SEBI from time to time. While sharing sensitive information, TLP shall be followed with four levels of sensitivity: white, green, amber, or red.

v. REs shall provide regular reports on the progress of the incident analysis.

b. Applicable to specified REs and MIIs

i. The Oversight SCOT of the stock exchanges and of the clearing corporations, the IT Strategy Committee of the depositories, and the internal Technology Committee of rest of the REs shall hold a meeting to discuss response plans, coordination with stakeholders for consistency in response actions, and information sharing for better awareness.

ii. If the cyber-attack is of high impact and had broad breach, then the RE has to do a press release and give a brief of incident, actions taken to recover, and normal operation resumption status (once achieved).

iii. If the cyber-attack is of low impact and had narrow breach, then REs has to inform all the affected customers / stakeholders.

4.3. RS.AN: Analysis

Analysis is conducted to ensure effective response and support recovery activities.

4.3.1. RS.AN: Objective:

a. Notifications from detection systems are investigated.
b. The impact of the incident is understood.
c. Forensics are performed.
d. Incidents are categorized consistent with response plans.
e. Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers).

4.3.2. RS.AN: Standard:

a. Detailed forensics and investigation of alerts and incident shall be done to prevent any such incidents.
b. RCA shall be done to determine the root cause of the attacks / incidents and to further enhance security posture to mitigate these kinds of attacks / incidents in future.

4.3.3. RS.AN: Guidelines:

a. Applicable to all REs

i. Alerts generated from monitoring and detection systems shall suitably investigated in order to determine activities that are to be performed to prevent spread of such incident of cyber-attack or breach, mitigate its effect and eradicate the incident.

ii. Data collection: REs shall collect and preserve data related to the incident, such as system logs, network traffic, forensic images of affected systems.

iii. Incident Analysis: Analyse the data to understand the scope, cause, and impact of the incident, including how the incident occurred, what systems and data were affected, and who was responsible.

iv. Evidence Preservation: Preserve evidence related to the incident, including digital artefacts, network captures, and memory dumps, in a secure and forensically sound manner.

v. Root Cause Analysis: Perform a root cause analysis (RCA) to identify the specific control that has failed, underlying cause of the incident and to identify potential areas of improvement.

vi. Forensic: Forensic analysis as per SEBI directions/SOP.

vii. Any incident of loss or destruction of data or systems shall be thoroughly analysed and lessons learned from such incidents shall be incorporated to strengthen the security mechanism and improve recovery planning and processes.

viii. Reporting: Create a detailed incident report that includes information on the scope, cause, and impact of the incident, as well as recommendations for improving incident response and recovery capabilities.

4.4. RS.IM: Improvements

Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

4.4.1. RS.IM: Objective:

a. Response plans are updated by incorporating lessons learned.

4.4.2. RS.IM: Standard:

a. Incorporate lessons learned from incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.

b. Communicate response plan changes to organization designated key personnel.

4.4.3. RS.IM: Guidelines:

a. Applicable to all REs

i. REs shall review bi-annually and update their response plan to strengthen their capability in the event of a future incident / attack.

5. RECOVERY

5.1. RC.PL: Recovery Planning

Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents. Recovery planning and processes are improved by incorporating lessons learned into future activities.

5.1.1. RC.PL: Objective:

a. Recovery plan is executed during or after a cybersecurity incident.

b. Recovery plans incorporate lessons learned.

c. Recovery strategies are updated.

5.1.2. RC.PL: Standard:

a. Recovery plan of REs shall have different scenarios based classifications.

b. Recovery Time Objective (RTO) and Recovery Point Objective (RPO) shall be mandated as specified by SEBI while executing recovery plan.

c. Drill for testing different recovery scenarios shall be conducted periodically[32].

5.1.3. RC.PL: Guidelines:

a. Applicable to all REs

i. The response and recovery plan of the REs shall have plans for the timely restoration of systems affected by incidents of cyber-attacks or breaches, for instance, offering alternate services or systems to Customers.

ii. In the event of disruption of any one or more of the 'Critical Systems', the RE shall, within 30 minutes of the incident, declare that incident as 'Disaster'. Accordingly, the RTO shall be two (2) hours as recommended by IOSCO[33]. The RPO shall be 15 minutes for all REs. The recovery plan shall be scenario-based and in line with the RTO and RPO specified. All REs shall comply with the mandated RTO and RPO for different scenarios attached as **Annexure-D**.

iii. An indicative (but not exhaustive and limited to) recovery plan to be followed by the REs has been attached as **Annexure-P**.

iv. All REs shall also conduct suitable periodic drills to test the adequacy and effectiveness of the aforementioned response and recovery plan.

5.2. RC.CO: Communications

Restoration activities are coordinated with internal and external parties (e.g. coordinating centres, Internet Service Providers, victims, other CSIRTs, and third-party service providers).

5.2.1. RC.CO: Objective:

a. Public relations are managed.

b. Reputation is repaired after an incident.

c. Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.

[32] Refer Table 10 in 'Framework Compliance, Audit, Report submission, and Timeline' section.

[33] Refer https://www.bis.org/cpmi/publ/d146.pdf.

5.2.2. RC.CO: Standard:

a. Actions taken during recovery process shall be informed to all related stakeholders.

5.2.3. RC.CO: Guidelines:

a. Applicable to all REs

i. Recovery plans shall be discussed within Oversight SCOT of the stock exchanges and of the clearing corporations, the IT Strategy Committee of the depositories, and the internal Technology Committee of rest of the REs. This plan shall include stakeholders' coordination in recovery process, and both internal and external communication.

E. Any other Suggestions/feedback regarding the consolidated Cybersecurity and Cyber Resilience Framework (CSCRF)

i. Considering the implication of the consolidated CSCRF on REs, public comments are invited on the proposed consolidated Cybersecurity and Cyber Resilience Framework (CSCRF). The comments/suggestions may be provided as per the format given below:

<table>
<tr><td colspan="5"><b>Name of the person/entity proposing comments:</b></td></tr>
<tr><td colspan="5"><b>Name of the organization (if applicable):</b></td></tr>
<tr><td colspan="5"><b>Contact details:</b></td></tr>
<tr><td colspan="5"><b>Category: whether market intermediary/participant (mention category/type such as Stock exchange, RTAs, stock broker etc.) or public (investor, academician, etc.)</b></td></tr>
<tr><td><b>Sr. No.</b></td><td><b>Extract from the consolidated CSCRF consultation paper (with details of page no., section no., clause)</b></td><td><b>Issues</b></td><td><b>Proposals / Suggestions / Changes</b></td><td><b>Rationale / Context / Remarks</b></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table>

ii. Comments, as per the aforementioned format, may be sent to SEBI by **July 25, 2023** through any of the following modes:

1. By email to: cscrf@sebi.gov.in
2. By post to the following address:

Ms. Shweta Banerjee (DGM-ITD)
SEBI Bhavan II BKC,
Plot no. C-7, ‘G’ Block, Bandra Kurla Complex,
Bandra (E), Mumbai (Maharashtra)- 400051

Issued on: July 04, 2023

Annexure-A: VAPT Report Format

REPORT FORMAT FOR MARKET ENTITIES TO SUBMIT THEIR COMPLIANCE AND FINDINGS REGARDING VAPT

NAME OF THE ORGANISATION:

ENTITY TYPE:

YEAR OF AUDIT:

CISO DETAILS:

NAME OF THE AUDITOR:

PLACED ON SCOT/ISSC DATE:

Authorised signatory declaration:

I/We hereby confirm that the information provided herein is verified by me/us and I/we shall take the responsibility and ownership of this VAPT report.

Signature:

Name of the signatory:

Designation (choose whichever applicable): MD / CEO / Board member / Partner / Proprietor

Company seal:

Table of Contents

Executive Summary

Scope of Audit

Sl. No.	Type of Assessment	List the details of the assessment
1.	Vulnerability Assessment of Infrastructure – Internal and External	//List the count of IPs audited
2.	Vulnerability Assessment of Applications – Internal and External	//List the count of IPs audited
3.	External Penetration Testing – Infrastructure and Applications	//List the count of IPs audited
4.	Internal Penetration Testing – Infrastructure and Applications	//List the count of IPs audited
5.	Wi-Fi Testing	//List the number of Wi-Fi access points/ routers/ devices audited
6.	Network Segmentation Testing	
7.	VA and PT of mobile Applications	//List the number of APK files and IPA files
8.	OS and DB Assessment	// List the type and number of OS and DBs audited.
9.	VAPT of Cloud Deployments	

Exclusions, if any:

// Please enclose attachments regarding exclusions as approved by SCOT/IT Strategy Committee/Technology Committee as per SEBI consolidated CSCRF.

Summary of the VAPT Report:

2.1. Details of Vulnerability Assessment findings:

Auditor for VA:										
Cert-in empanelled:										
VA Start Date:										
VA End Date:										
Scope	Vulnerability Assessment									Remarks
	Identified vulnerabilities				Closure Timelines	Open vulnerabilities (Will be applicable during final submission)				
	High/ Critical	Medium	Low	Total		High/ Critical	Medium	Low	Total	
Critical Assets										
VA of infrastructure - Internal and External										
VA of Applications - Internal and External										
WiFi Testing										

Network Segmentation										
VA of mobile applications										
OS and DB Assessment										
VA of cloud deployments										
Exclusions, if any										

2.2. **Details of Penetration Testing findings:**

Auditor for PT:										
Cert-in empanelled:										
PT Start Date:										
PT End Date:										
Scope	Penetration Testing									Remarks
	Identified vulnerabilities				Closure Timelines	Open vulnerabilities (Will be applicable during final submission)				
	High/ Critical	Medium	Low	Total		High/ Critical	Medium	Low	Total	
Critical Assets										
External Penetration Testing - Infrastructure and Application										
Internal Penetration Testing - Infrastructure and Application										
PT of mobile applications										
PT of cloud deployments										

Exclusions, if any										

3. **Detailed Report**

Detailed report to be submitted for all the items in the scope as per the below mentioned format (to be submitted when sought by SEBI):

Sr. No	URL / Application Name	Type of Risk	Observations / Vulnerability	Reference (CVE/ Best Practise)	Impact	Recommendations	Management Comments with specific closure timelines
2.							
…							

Annexure-B: Audit Metrics

Audit Metrics

An indicative (but not limited to) list of metrics that would help to analyse materiality are given by ISACA IS Auditing Guidelines G6[34]:

S. No.	Audit metrics
1.	Criticality of the business processes supported by the system or operation
2.	Criticality of the information databases supported by the system or operation
3.	Number and type of application developed
4.	Number of users who use the information systems
5.	Number of managers and directors who work with the information systems classified by privileges
6.	Criticality of the network communications supported by the system or operation
7.	Cost of the system or operation (hardware, software, staff, third-party services, overheads or a combination of these)
8.	Potential cost of errors (possibly in terms of lost sales, warranty claims, irrecoverable development costs, cost of publicity required for warnings, rectification costs, health and safety costs, unnecessarily high costs of production, high wastage, etc.)
9.	Cost of loss of critical and vital information in terms of money and time to reproduce
10.	Effectiveness of countermeasures
11.	Number of accesses/transactions/inquiries processed per period
12.	Nature, timing and extent of reports prepared and files maintained
13.	Nature and quantities of materials handled (e.g., where inventory movements are recorded without values)

[34] Refer Para 3.1.10: https://cs.uns.edu.ar/~mc/ADS/downloads/Material%20Complementario/Material%20modulo%202/isaca%20guidelines/G6-Materiality-Concepts-6Mar08.pdf

14.	Service level agreement requirements and cost of potential penalties
15.	Penalties for failure to comply with legal, regulatory and contractual requirements

Annexure-C: Cyber Audit Report Format

Cyber audit report format for compliance submission

NAME OF THE ORGANISATION:

ENTITY TYPE:

YEAR OF AUDIT:

CISO DETAILS:

PLACED ON SCOT/ISSC DATE:

Authorised signatory declaration:

I/We hereby confirm that the information provided herein is verified by me/us and I/we shall take the responsibility and ownership of this cyber audit report.

Signature:

Name of the signatory:

Designation (choose whichever applicable): MD / CEO / Board member / Partner / Proprietor

Company seal:

1. Background

2. Details of Auditee

3. Audit Team Member Details

Auditor name	
Auditor address	
Contact information	
Location of audit	
Audit team members and details of qualifications	

4. Scope of audit/Terms of reference (as agreed between the auditee and auditor), including the standard/specific scope for audit:-

   a) Audit Period –

   b) Date of agreement between MII and auditor

   c) Engagement period-

   d) List of SEBI Circulars and Advisories covered:

      ---

   e) List of all IT infrastructure (including IT systems of PDC, DR, Near site, Co-lo facility) covered under audit

      ---

   f) Geographical locations covered under audit (PDC/DR/near site)

   g) VAPT (Vulnerability assessment and penetration testing)

   h) Any other specific item(s)

5. Methodology /Audit approach (audit subject identification, pre-audit planning, data gathering methodology, sampling methodology etc. followed)

6. Executive Summary of findings (including identification tests, tools used and results of tests performed)

S.No	Number of Non-conformity	Number of observations	Risk rating			Any other comments
			High	Medium	Low	
1						

7. Control-wise Compliance status of this SEBI consolidated CSCRF

S.No	Audit Period	Control prescribed by SEBI (Clause number and text)	*List of documentary evidence including physical inspection/sample size taken by the auditor	Description of the finding	Compliance status	Risk Category of non-compliance	Auditor recommendations / Corrective actions if non-compliance	Deadline of corrective action	Management response in case of acceptance of associated risks	Whether similar issue was reported in the last three years.
1										
2										
…										
N										

*Explicit reference to the key auditee organisational documents (by date or version) including policy and procedure documents

*Audit report should provide terms of reference of audit which shall indicate the scope/perimeter of the coverage of the systems audited in the cyber audit report regarding the compliances checked including areas but not limited to computer hardware, business applications, software, cyber governance, linkage with vendor systems like RTAs, Fund Accountants, email systems etc.

*Audit report should include open observations from previous audits and comments of auditors for compliances checked for the same.

* The auditor shall mention in the audit report the methodology adopted to check compliance and the reason for disagreement between auditor and management, if any shall be recorded in audit report.

8. Format for exception reporting by the RE:

S. No.	Reported Entity	Period of cyber Audit	Non-compliance clause of consolidated CSCRF for AMCs	Text of non-compliance	Auditor observation	Auditor recommendation	Management comments	Comments of Board of RE	Comments of Board of Trustee	Status of non-compliance (open/closed)	Name of auditor	Auditor eligibility	Repeat observation in last 3 audits	Deadline for corrective action	Risk category of non-compliance
												CERT			
												CERT			
												CERT			

9. Details of findings (including analysis of vulnerabilities/issues of concern and recommendation for action)

Description of finding (a)	
Name of system belongs to MII or third party vendor (b)	
Status/nature of findings (c)	
Risk rating of finding by auditor (d)	
C/I/A effected (e)	
Clause No. of SEBI cybersecurity framework/advisory violated (f)	
Test cases used (g)	
Impact analysis (h)	
Root Cause analysis (i)	
Corrective Action proposed by auditor (j)	
Deadline for corrective action (k)	
Management response (l)	
Whether Similar Issue was observed in any of previous 3 audit (m)	
List of Documentary evidence verified during review/audit (n)	

a) Description of findings/observations – Description of the findings in sufficient details, referencing any accompanying evidence
b) Name of system belongs to MII or vendor-(Self Explanatory term)
c) Status/ Nature of Findings – The category can be specified, for example:

   a. Non-compliant (Major/Minor)
   b. Work in progress
   c. Observation

d) Risk Rating of finding - A rating has to be given for each of the observations based on its impact and severity to reflect the risk exposure as well as the suggested priority for action

Rating	Description
HIGH	Represents weakness in control with respect to threat(s) that is /are sufficiently capable and impacts asset (s) leading to regulatory non-compliance, significant financial, operational and reputational loss. These observations need to be addressed with utmost priority.
MEDIUM	Represents weakness in control with respect to threat(s) that is /are sufficiently capable and impacts asset (s) leading to exposure in terms of financial, operational and reputational loss. These observations need to be addressed reasonable timeframe.
LOW	Represents weaknesses in control, which in combination with other weakness can develop into an exposure. Suggested improvements for situations not immediately/directly affecting controls. .

e) C/I/A**-**Principle of Confidentiality/integrity/availability affected due to issued left unaddressed**.**
f) Clause No. of SEBI Cybersecurity circular/advisory violated**-**The clause corresponding to this observation w.r.t to SEBI circular on Cybersecurity/advisories issued by SEBI.
g) Test cases used **–**The details of test cases used for arriving at this observation, provide annexure numbers in case of detailed test cases.
h) Impact Analysis **–** An analysis of the likely impact on the operations/ activity of the organization
i) Root Cause analysis – A detailed analysis on the cause of the non-conformity.
j) Corrective Action proposed by auditor **–** The action taken to correct the non-conformity
k) Deadline for corrective action**-**The auditor should specify the deadline not only for the corrective action on the system where NC/observation was found, but also specify the deadline for corrective action on systems where similar observations could have been found/are found
l) Management response
m) Whether Similar Issue was observed in any of previous 3 audit
n) List of Documentary evidence verified during review/audit

10. Specific best practices implemented by the auditee in generalized manner without infringing on Intellectual Property Rights (IPRs)

11. Any other comments by auditor

12. Conclusion of cyber audit

Annexure-D: Scenario-based RTO/RPO

Cybersecurity scenario-based RPO/RTO

Scenarios which are targeted to cover in Cyber Response plan as well as Cyber Resiliency Testing (Types of Attack × Potential Targeted Time intervals- On Core Systems):

	Cyber Attack-> Time Interval	DDoS	Malware/Malicious Code Attack	Application Level Attacks (SaaS Model)	DNS Based Attacks (Internal & Internet)	Brute Force/Authentication based attack	AD attack
Pre-open Sessions	Before BOD/early Morning						
	Before 9:00 hrs						
	B/W 9:00 - 9:15 hrs						
Regular Trading Sessions	09:15 - 15:30 hrs						
Closing Session	15:30 -16:00 hrs						
	Post 16:00 hrs						

Attack Scenario Category	Types of attacks	Impact	Response & Recovery
DDOS		Service Unavailability	DDOS Protection services for auto mitigation.
Malware Attacks	Ransomware	Service Unavailability, Data Corruption, Data exfiltration, Website Defacement	1. Isolate and contain the infected systems from overall network. Block IOCs, DNS traffic.
	Spyware		2. Restrict administrative and system access.
	Trojans		3. Monitor network traffic.
	Worms		4. Restore OS, application and data from existing backups.
	Bots		
Application Level Attacks	Injection	Service Unavailability, Website Defacement	1. Monitor network traffic and logs.
	Broken Authentication & Session Management		2. Disable suspected user accounts and change access credentials.

Attack Scenario Category	Types of attacks	Impact	Response & Recovery
	Cross-Site Scripting/request forgery		3. Apply patches/changes for vulnerability.
DNS Based Attacks	DNS Spoofing/Cache Poisoning	Service Unavailability	1. Analyse the traffic requests.
	DNS Flood Attack		2. Restore DNS entries
	DNS Encoding		3. Monitor the DNS requests and responses
Social Engineering Attacks	Phishing	It is a method, It may lead to any of the other attack	Spam filtering policy should be configured in available tools as a precaution.
Watering hole		Service Unavailability	1. Coordination with respective agency/website owner.
			2. Isolation of affected systems.
			3. Clean/replace the affected system.
Brute Force	Trial and Error approach	Service Unavailability	1 Proper account locking mechanism.
	Authentication Based Attack		2 Monitoring

Attack Scenario Category	Types of attacks	Impact	Response & Recovery
Active Directory Attack	Inappropriate access.	Data Confidentiality, compromised user accounts	1.Review default security settings.
			2.Least privilege in AD roles.

Annexure-E: Guidelines on Outsourcing of Activities

SEBI’s ‘Guidelines on Outsourcing of Activities by Intermediaries’ circular will be attached here.

https://www.sebi.gov.in/legal/circulars/dec-2011/guidelines-on-outsourcing-of-activities-by-intermediaries_21752.html

Annexure-F: Application Authentication Security

Illustrative Measures for Application Authentication Security are given below:

1. Any Application offered by REs to Customers containing sensitive, private, or critical data such as IBTs, SWSTs, Back office etc. referred to as “Application” hereafter) over the Internet should be password protected. A reasonable minimum length (and no arbitrary maximum length cap or character class requirements) should be enforced. While it is difficult to quantify password “complexity”, longer passphrases have more entropy and offer better security in general. REs should attempt to educate Customers of these best practices.

2. Passwords, security PINs etc. should never be stored in plain text and should be one-way hashed using strong cryptographic hash functions (e.g.: bcrypt, PBKDF2) before being committed to storage. It is important to use one-way cryptographic hashes to ensure that stored password hashes are never transformed into the original plaintext values under any circumstances.

3. For added security, a multi-factor (e.g.: two-factor) authentication scheme may be used (hardware or software cryptographic tokens, VPNs, biometric devices, PKI etc.). In case of IBTs and SWSTs, a minimum of two-factors in the authentication flow are mandatory.

4. In case of Applications installed on mobile devices (such as smartphones and tablets), a cryptographically secure biometric two-factor authentication mechanism may be used.

5. After a reasonable number of failed login attempts into Applications, the Customer’s account can be set to a “locked” state where further logins are not possible until a password and authentication reset is performed via an out-of-band channel validation, for instance, a cryptographically secure unique link that is sent to the Customer’s registered e-mail, a random OTP (One Time Password) that is sent as an SMS to the Customer’s registered mobile number, or manually by the Broker after verification of the Customer’s identity etc.

6. Avoid forcing Customers to change passwords at frequent intervals which may result in successive, similar, and enumerated passwords. Instead, focus on strong multi-factor authentication for security and educate Customers to choose strong passphrases. Customers may be reminded within reasonable intervals to update their password and multi-factor credentials, and to ensure that their out-of-band authentication reset information (such as e-mail and phone number) are up-to-date.

Both successful and failed login attempts against a Customer’s account may be logged for a reasonable period of time. After successive login failures, it is recommended that measures such as CAPTCHAs or rate-limiting be used in Applications to thwart manual and automated brute force and enumeration attacks against logins.

Annexure-G: Data Security on Customer Facing Applications

Illustrative Measures for Data Security on Customer Facing Applications are given below:

1. Analyse the different kinds of sensitive data shown to the Customer on the frontend application to ensure that only what is deemed absolutely necessary is transmitted and displayed.
2. Wherever possible, mask portions of sensitive data. For instance, rather than displaying the full phone number or a bank account number, display only a portion of it, enough for the Customer to identify, but useless to an unscrupulous party who may obtain covertly obtain it from the Customer's screen. For instance, if a bank account number is "123 456 789", consider displaying something akin to "XXX XXX 789" instead of the whole number. This also has the added benefit of not having to transmit the full piece of data over various networks.
3. Analyse data and databases holistically and draw out meaningful and "silos" (physical or virtual) into which different kinds of data can be isolated and cordoned off. For instance, a database with personal financial information need not be a part of the system or network that houses the public facing websites of the REs. They should ideally be in discrete silos or DMZs.
4. Implement strict data access controls amongst personnel, irrespective of their responsibilities, technical or otherwise. It is infeasible for certain personnel such as System Administrators and developers to not have privileged access to databases. For such cases, take strict measures to limit the number of personnel with direct access, and monitor, log, and audit their activities. Take measures to ensure that the confidentiality of data is not compromised under any of these scenarios.
5. Use industry standard, strong encryption algorithms (eg: RSA, AES etc.) wherever encryption is implemented. It is important to identify data that warrants encryption as encrypting all data is infeasible and may open up additional attack vectors. In addition, it is critical to identify the right personnel to be in charge of, and the right methodologies for storing the encryption keys, as any compromise to either will render the encryption useless.
6. Full-disk Encryption (FDE) for protecting sensitive data-at-rest at the hardware level by encrypting all data on a disk drive shall be used wherever possible. File-based Encryption (FBE) encrypts specific files or directories instead of the complete data on a disk. Therefore, both FDE and FBE with strong industry-standard algorithms shall be used together.
7. Ensure that all critical and sensitive data is adequately backed up, and that the backup locations are adequately secured. For instance, on servers on isolated networks that have no public access endpoints, or on-premise servers or disk drives that are off-limits to unauthorized personnel. Without up-to-date backups, a meaningful recovery from a disaster or cyber-attack scenario becomes increasingly difficult.

Annexure-H: Data Transport Security

Illustrative Measures for Data Transport Security are given below:

1. When an Application transmitting sensitive data communicates over the Internet with RE's systems, it should be over a secure, encrypted channel to prevent Man-In-The-Middle (MITM) attacks, for instance, an IBT or a Back office communicating from a Customer's web browser or Desktop with the RE's systems over the internet, or intra or inter organizational communications. Strong transport encryption mechanism such as TLS (Transport Layer Security, also referred to as SSL) should be used.

2. For Applications carrying sensitive data that are served as web pages over the internet, a valid, properly configured TLS (SSL) certificate on the web server is mandatory, making the transport channel HTTP(S).

3. Avoid the use of insecure protocols such as FTP (File Transfer Protocol) that can be easily compromised with MITM attacks. Instead, adopt secure protocols such as FTP(S), SSH and VPN tunnels, RDP (with TLS) etc.

Annexure-I: Framework for Adoption of Cloud Services

SEBI's 'Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs)' circular will come over here.

https://www.sebi.gov.in/legal/circulars/mar-2023/framework-for-adoption-of-cloud-services-by-sebi-regulated-entities-res-_68740.html

Annexure-J: Cyber Capability Index (CCI)

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). MIIs are directed to conduct self-assessment of their cyber resilience using the index, on a quarterly basis, starting from the quarter ending September 2019.

B. **Index Calculation Methodology**-

1. The index is calculated on the basis of 24 parameters extracted from NIST publication *'Performance Measurement Guide for Information Security'*[35]. These parameters have been given different weightages on the basis of suggestions provided by HPSC-CS.

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

[35] Refer https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-55r1.pdf

S No.	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage
1.	Security Budget Measure	Information Security Goal: Provide resources necessary to information and information systems.	Percentage (%) of the organisation information system budget devoted to information security.	Impact	(Information security budget/total organisation information technology budget) *100	12%	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	Objective of this measure to ensure the vulnerabilities in organization's system are identified and mitigated	Percentage of vulnerabilities mitigated pertaining to organization in a specified time frames.	Effectiveness Measure	(Number of vulnerabilities mitigated/Number of vulnerabilities identified)*100	100 %	1. Confirmation that VAPT is done by CERT-In empanelled auditor and as per the scope prescribed by SEBI 2. VAPT report summary and its closure report. 3. Time taken to close the	12%

S No.	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage
							vulnerabilities identified.	
3.	Security Training Measure	Information Security Goal: Ensure that organization personnel are adequately trained to carry out their assigned information security- related duties and responsibilities	Percentage (%) of information system security personnel that have received security training.	Implementation	(Number of information system security personnel that have completed within the past year/total number security training of information system security personnel) *100	100 %	1. Details of the training/awareness session scheduled within past 1 year. 2. Cyber audit observation against clause 2.2 of the SEBI master framework.	5%

S No.	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage
4.	Remote Access Control Measure	Information Security Goal: Restrict information, system, and component access to individuals or machines that are identifiable ,known, credible, and authorized.	Percentage (%) of remote access points used to gain unauthorized access.	Effectiveness	(Number of remote access points used to gain unauthorized access/to access points) *100	0%	1. Does the organization use automated tools to maintain an up-to-that identifies all remote access points? 2. How many remote access points exist in the organization's network? 3. Does the organisation employ intrusion detection systems (IDS) to monitor traffic traversing remote access points? 4. Does the organisation collect and review audit logs associated with all remote access points?	2%

S No.	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage
							5. Does the organization maintain a security incident database that identifies standardized incident categories for each incident? 6. Based on reviews of the incident database, IDS 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?	

S No.	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage
5.	Audit Record Review Measure	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, or inappropriate activity.	Average frequency of audit records review and analysis for inappropriate activity.	Efficiency	Average frequency during reporting period.	Daily	1.Is logging activated on the system? 2.Does the organization have clearly defined criteria for what constitutes evidence of "inappropriate" activity within system audit logs? 3. For the reporting period, how many system audit logs have been reviewed within past one month to six months for inappropriate activity.	2%

S No.	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage
6.	C&A (Certification & Accreditation) Completion Measure	Information Security Goal: Ensure all information systems have been certified and accredited as required	Percentage (%) of new systems that have completed certification and accreditation (C&A) prior to their implementation.	Effectiveness	(Number of new systems with complete C&A packages with Authorizing Official approval prior to implementation) /(total number of new systems)* 100	100 %	1. Does your organization maintain a complete and up to date system inventory? 2. Is there a formal C & A process within organization? 3. If the answer to question 2 is yes, are system development projects required to complete C & A prior to implementation? 4. How many new systems have been implemented during the reporting period? 5. How many systems indicated in question 4 have	2%

S No.	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage
							received an authority to operate prior to implementation?	

S No.	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage
7.	Configuration Changes Measure	Information Security Goal: Establish and maintain baseline configuration and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	Percentage (%) approved and implemented configuration changes identified in the latest automated baseline configuration.	Implementation	(Number of approved and implemented configuration changes identified in the latest automated baseline configuration/total number of configuration changes identified through automated scans) * 100	100 %	1. Does the organization manage configuration changes to information systems using 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	2%

S No.	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage
							last reporting period? 4. How many change control requests were approved and implemented over the last reporting period? 5. Cyber audit observation against clause 2.1.3.V of the SEBI master framework.	

S No.	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage
8.	Contingency Plan Testing Measure	Information Security Goal: Establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for 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 annual contingency plan testing.	Effectiveness	(Number of information systems that have conducted annual contingency plans testing/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 year ?	4%

S No.	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage
9.	User Accounts Measure	Information Security Goal: All system users are identified and authenticated in accordance with information security policy.	Percentage (%) of users with access to shared accounts.	Effectiveness	(Number of users with access to shared accounts/total number of users) *100	0%	1. Organization should have a documented and approved access control mythology 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 clause 2.1.3.i.a of SEBI master framework.	3%

S No.	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage
10.	Incident Response Measure	Information Security Goal: Track, document, and report incidents to appropriate organizational officials and/or authorities.	Percentage (%) of incidents reported within required time frame per applicable incident category (the measure will be computed for each incident category described in Implementation Evidence).	Effectiveness	For each incident category (number of incidents reported on time/total number of reported incidents) *100	100 %	1. How many incidents were reported during the period- Category 1 - Unauthorized Access? Category 2 - Denial of Service? Category 3 - Malicious Code? Category 4 - Improper Usage? Category 5 - Scans/Probes/Attempted Access? 2. Of the incidents reported, how many were reported within the prescribed time frame for their category, according to the time frames established by	5%

S No.	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage
							CERT-In Category 1 - Unauthorized Access? Category 2 - Denial of Service? Category 3 - Malicious Code? Category 4 - Improper Usage? Category 5 - Scans/Probes/Attempted Access?	

S No.	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage
11.	Maintenance Measure	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 formal maintenance schedules.	Efficiency	(Number of system components that undergo maintenance according to formal maintenance schedules/total number of system components) *100	100 %	1. Does the system have a formal maintenance schedule? 2. How many components are contained within the system? 3. How many components underwent maintenance in accordance with the formal maintenance schedule?	2%
12.	Media Sanitization Measure	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 tested) * 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	2%

S No.	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage
							observation against clause 2.1.3.c.iii of the SEBI master framework.	
13.	Physical Security Incidents Measure	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	1%

S No.	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage
							systems? 4. Cyber audit Observation against clause 2.1.3.a.iii of SEBI master framework.	
14.	Planning Measure	Information Security Goal: Develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for information systems, and the rules of behaviour for individuals accessing these systems	Percentage of employees who are authorized access to information systems only after they sign an acknowledgement that they have read and understood rules of behaviour.	Implementation	(Number of users who are granted system access after signing rules of behaviour/total number of users with system access) *100	100 %	1. How many users access the system? 2. How many users signed rules of behaviour acknowledgements? 3. How many users have been granted access to the information system only after signing rules of behaviour acknowledgements?	1%

S No.	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage
15.	Personnel Security Screening Measure	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.	Implementation	(Number of individuals screened/total number of individuals with access) *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%
16.	Risk Assessment Measure	Objective of this measure to periodically assess the risk to organization's IT assets and operations.	Percentage of risks mitigated pertaining to organization in a specified time frames.	Implementation Measure	(Number of risks mitigated /number of risks associated with critical assets)*100	100 %	1. Risks associated with critical assets. 2. Mitigation of risks identified. 3. Cyber Audit observation against this clause 1.2.3.a.iii-(a) of SEBI master framework.	5%

S No.	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage
17.	Service Acquisition Contract Measure	Information Security Goal: Ensure third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.	Percentage (%) of system and service acquisition contracts that include security requirements and/or specifications.	Implementation	(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.Cyber Audit Observation against clause 1.1.3.a.vi of the SEBI master framework.	3%
18.	System and Communication Protection Measure	Information Security Goal: Allocate sufficient resources to adequately protect electronic information infrastructure.	Percentage of mobile computers and devices that perform all cryptographic operations.	Implementation	(Number of mobile computers and devices that perform all cryptographic operations /total number of	100 %	1. How many mobile computers and devices are used in the organization? 2. How many mobile computers and devices	1%

S No.	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage
					mobile computers and devices) *100		employ cryptography? 3. How many mobile computers and devices have cryptography implementation waivers?	
19.	System and Information Integrity	Information Security Goal: Provide protection from malicious code at appropriate locations within organizational information systems, monitor information systems security alerts and advisories, and take appropriate actions in response.	Percentage (%) of operating system vulnerabilities for which patches have been applied or that have been otherwise mitigated.	Effectiveness	(Number of vulnerabilities addressed in distributed alerts and advisories for which patches have been implemented, determined as non-applicable, or granted a waiver/total number of applicable vulnerabilities identified through alerts and advisories	100 %	1. Does the organization distribute alerts and advisories? 2. How many vulnerabilities were identified by analysing distributed alerts and advisories? 3. How many vulnerabilities were identified through vulnerability scans? 4. How many patches or work-around were	8%

S No.	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage
					and through vulnerability scans) *100		implemented to address identified vulnerabilities? 5. How many vulnerabilities were determined to be non-applicable? 6. How many waivers have been granted for weaknesses that could not be remediated by implementing patches or work-around?	
20.	Critical Assets Identified	Objective of this measure to encourage the MIIs to include their assets into category of critical assets.	Percentage (%) of the critical identified systems by MIIs among all other IT systems.	Implementation Measure	(Number of Critical System Identified/Total IT systems in organization) *100	50%	1. Process to identify list of critical assets. 2. Indicative list of critical identified assets. 3. Approval of the list of critical assets identified by Board of MIIs. 4. Proofs	10%

S No.	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage
							establishing list of critical assets are being reviewed continuously. 5. Cyber Audit Observation against this clause 1.1.3.a.i of SEBI master framework.	
21.	Cybersecurity principles (prescribed by NCIIPC) encompassed in policy. (Based on clause-4 of SEBI circular)	Objective of this measure to improve the quality of the cybersecurity policy document of the MIIs	Percentage of the principles (prescribed by NCIIPC) incorporated in policy document.	Implementation Measure	(Principles incorporated in organization's policy from NCIIPC/Total principles prescribed by NCIIPC)*100	100 %	1. Mappings between Principles prescribed by NCIIPC and cybersecurity Policy Document of MIIs. 2. Cyber Audit Observation against this clause 1.2.3.c.i of SEBI master framework.	1%
22.	CSK Events	Objective of this measure to mitigate threats upon external IPs	Number of events reported by CSK.	Effectiveness Measure	Number of events reported by CSK to the organization.	0	1. Summary report of the events reported by CSK.	4%

S No.	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage
23.	Cyber Audit Observations	Create, protect, and retain cyber audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate activity.	Percentage (%) of guidelines clauses (pertaining to SEBI cybersecurity master framework) the organization is non-`compliant or partially compliant.	Effectiveness Measure	(Number guidelines clauses the organization is non-compliant or partially compliant/Total number of clauses).	0%	1. Frequency of cyber audits in a year. 2. Policy/procedure to conduct cyber audit. 3. Terms of reference of the cyber audit. 4. Cyber audit report with aggregate summary and observations. 5. Evidence against each of the clause along with auditor's comments.	12%
24.	Cybersecurity Policy Document	Develop, document, periodically update, and implement cybersecurity policies and procedures for organizational information systems that describe the security controls in			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 clause 1.2.3.a.i of the circular.	4%

S No.	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage
		place or planned for information systems.						

3. Based on the value of the index, the cybersecurity maturity level of the MIIs shall be determined as follows:

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

Annexure-K: 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 (not limited to) like 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.	Internal Penetration Testing-Infrastructure & Application
5.	WIFI Testing
6.	Network Segmentation
7.	VA & PT of Mobile applications
8.	OS & DB Assessment
9.	VAPT of Cloud implementation and deployments

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 consolidated 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

Annexure-L: Cyber-SOC Framework for MIIs

SEBI's 'Cyber-SOC Framework for MIIs' circular will be attached here.

https://www.sebi.gov.in/legal/circulars/dec-2018/cyber-security-and-cyber-resilience-framework-of-stock-exchanges-clearing-corporations-and-depositories_41244.html

Annexure-M: Functional Efficacy of SOC

Measuring and auditing functional efficacy of SOC

1. SEBI has formulated a quantifiable method with various domains / sub-domains to measure functional efficacy of SOC.
2. As SEBI has prescribed a weightage for the domains / sub-domains with an overall weightage of 80%, it gives REs necessary leeway to add other new domains/sub-domains or adjust the weightage of each existing domain/sub-domain to be equivalent to or greater than the minimum weightage to make total weightage 100%, depending on their IT environment and infrastructure. All REs are required to report their SOC efficacy to SEBI along with the compliance reports and audit reports of this circular.

   2.1. Following are domains and their respective minimum weightage for measuring functional efficacy of SOC:

S. No.	Domain	Minimum Weightage
1	Network	10%
2	Data Protection	10%
3	Perimeter	10%
4	Access Control	15%
5	Edge	5%
6	Endpoint	15%
7	Threat Intel	5%
8	Hosts	10%
Overall		80%

   2.2. For each of the domains listed above, following are the sub-domains and their respective minimum weightage:

S. No.	Area / Sub-domain	Minimum Weightage
1	Policy Compliance	15%
2	Environment Coverage	15%
3	Preventive Effectiveness	15%
4	Detective Effectiveness	15%
5	Resiliency of Solution	20%
Overall		80%

3. To measure SOC efficacy from governance perspective, it is also mandated to create three categories namely mandatory (must have), desirable (as per the nature of the organization) and good to have (i.e. with respect to future preparedness).

SN.	Category	Parameters	Response (Yes/No)	Evidences (if response provided is Yes)
1		Whether there is an approved cybersecurity policy and the corresponding Standard Operating Procedures (SOPs) in place?		
2		Whether VAPT is conducted regularly (in-line with the requirement provided in *cybersecurity circulars/ advisories issued by SEBI)?		
3		Whether the vulnerabilities identified (during VAPT exercise or otherwise) are categorized, and closed within the prescribed timeline (as per the requirements provided in *cybersecurity circular/ advisory issued by SEBI)?		
4		In the event vulnerabilities have not been closed within the prescribed timelines or the vulnerabilities cannot be closed, whether any compensating controls have been put in place?		
5		Whether cybersecurity audit (if applicable) and systems audit are conducted regularly?		
6		Whether the observations identified in audits (cybersecurity audit and IT audit) are closed within the prescribed timelines		

		(as per requirements provided in* SEBI circular/ advisory/ regulation)?		
7		Whether monitoring through SOC is done round-the-clock throughout the year?		
8		Whether Indicators of Compromise (IOCs) are processed by SOC (i.e. IOCs are received regularly through feeds/ updates, IOCs are updated in all applicable security devices, actions are taken in the event an IOC is found in network, etc.)?		
9		Whether qualified personnel are deployed in SOC (i.e. detection, response and threat hunting capability of the SOC personnel)?		
10	Desirable	Whether any benefits/ value addition has been observed through implementation of SOC?		
11		Whether inputs are received in the form of threat alerts/ threat intelligence regularly? Whether action is taken on such inputs?		
12		Whether the SOC rules and use cases/ scenarios have been created to detect and respond to all relevant signature based and behaviour-based attacks keeping the latest attack techniques also in mind?		

13		What is the quality of logs ingested in SOC? i.e. i. What is the source i.e. which devices, OS, databases, etc. are sending logs? ii. What is the frequency of logs? iii. What is the verbosity of logs?		
14		Whether ISO 27001 certification has been obtained?		
15		Whether security devices/ controls are present for monitoring of network traffic as well as endpoints?		
16		Whether drills (cyber drills, DC-DR, etc.) are conducted regularly (as per the requirement provided in *SEBI circular/ advisory/ regulation)?		
17		Whether new technologies such as Artificial Intelligence (AI)/ Machine Learning (ML) are utilized in correlation and forecasting?		
18	Good to Have	Whether red team exercise (automated or manual) is undertaken regularly?		
19		Whether Indicators of Attack (IOAs) are processed by SOC (i.e. IOAs are detected, updated, acted upon, etc.)		

20		Whether attack surface monitoring is conducted regularly?		
21		Whether SOC2 certification has been obtained?		

All REs are required to send responses to parameters given above to measure SOC efficacy from governance perspective.

The baseline for these categories as well as inclusion of other parameters (for auditing SOC efficacy) may be updated on the basis of feedback/ inputs received during the auditing process.

Annexure-N: Incident Classification

Guidelines on Classification of Incidents

Incident[36]: Any adverse event or the threat of such an event on a RE's and/ or its Third Party Service Provider's (TPSP) information systems or networks that results in or could result in misuse/ compromise/ damage/ destruction of (i) information assets of the RE and/ or (ii) the physical infrastructure and/or environment hosting the information assets of the RE; in terms of confidentiality, integrity and availability, shall be considered as an incident.

Threshold for classifying incidents:

Incidents that require to be reported[37]:

a. Incidents that compromises or attempts to compromise the confidentiality or integrity of RE's data/ information stored/ processed in the information assets of RE and/ or its Third-party service providers. The following types of incidents needs to be reported but not necessarily limiting to
   i. Targeted scanning/ probing of critical network systems
   ii. Compromise of critical systems/information
   iii. Unauthorized access of IT systems/ data
   iv. Defacement of website or intrusion into a website and unauthorized changes such as inserting malicious code, link to external websites etc.
   v. Malicious code attacks such as spreading of virus/worm/ Trojan/ Bots/ Spyware/ Ransomware/Crypto miners
   vi. Attack on servers such as Database, Mail, DNS and network devices such as routers.
   vii. Identity theft, spoofing and phishing attacks
   viii. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.
   ix. Attacks on Critical infrastructure and operational technology systems and wireless networks.
   x. Attacks on Applications
   xi. Data breach
   xii. Data leak
   xiii. Attacks on Internet of Things (IoT) devices and associated systems, networks, software, servers
   xiv. Attacks through malicious mobile apps.
   xv. Attacks or incident affecting Digital Payment Systems.
   xvi. Unauthorized access to social media accounts.
   xvii. Attacks or malicious// suspicious activities affecting cloud computing systems/servers/software/applications.

[36] Incident definition taken from RBI's guidelines on Reporting of unusual cybersecurity incidents for unified approach of incident response and management in banking sector and securities market.

[37] Refer Cert-IN direction No. 20(3)/2022 dated April 28, 2022

xviii. Attacks or malicious suspicious activities affecting systems/ servers/ networks/ software/ applications related to Big Data, Block Chain, virtual assets, virtual asset exchanges, custodian wallets, robotics etc.

xix. Attacks or malicious/ suspicious activities affecting systems/ servers/ software/ applications related to Artificial Intelligence and Machine Learning.

xx. Any new type of attack not necessarily falling into one of the above.

Incidents that are not required to be reported under unusual cyber incident[38]:

a. Instances of phishing/vishing at customer's end.
b. Security alerts/ events that are not materializing into an incident.
c. DoS/ DDoS attack not lasting beyond 30 minutes contiguously or not impacting the customer service even if it lasts beyond 30 minutes.
d. Phishing websites, rogue apps that are monitored/ brought down on an ongoing basis.
e. Vulnerabilities observed or brought to the notice of the Regulated Entity which is neither an attempt nor a successful incident.
f. Connectivity issues.

1. Cybersecurity incidents may be classified into the following four categories:
   1. Low Severity
   2. Medium Severity
   3. High Severity
   4. Critical Severity

2. The parameters for classification of the incidents are as follows:

Sr. No.	Category	Details
1	Low	System probes or scans detected on external systems; intelligence received concerning threats to which systems may be vulnerable; intelligence received regarding username password compromise; isolated instances of known malwares easily handled by antivirus software, etc.
2	Medium	Target recon or scans detected; penetration or denial of service attacks attempted with no impact on operations; widespread instances of known malwares easily handled by antivirus software; isolated instances of a new malwares not handled by anti-virus software; instances of phishing emails; instances of data corruption, modification and deletion being reported, etc.
3	High	Penetration or denial of service attacks attempted with limited impact on operations; widespread instances of a new malwares not handled by anti-virus software; unauthorized access to servers and network devices;

[38] Refer RBI's guidelines on Reporting of unusual cybersecurity incidents for unified approach of incident response and management in banking sector and securities market.

		unauthorized or unexpected configuration changes on network devices detected; impersonation of SEBI officials in email communications; Data Exfiltration; unusually high count of phishing emails; instances of outbound phishing emails; some risk of negative financial or public relations impact, etc.
4	Critical	Successful penetration or denial of service attacks detected with significant impact on operations; ransomware attack; Exfiltration of market sensitive data; widespread instances of data corruption causing impact on operations; Significant risk of negative financial or public relations impact, etc.

3. Any incident that results in disruption, stoppage or variance in the normal functions/operations of systems of the entity thereby impacting normal/regular service delivery and functioning of the entity, must be classified as High or Critical incident.

Annexure-O: SOPs for handling Cybersecurity Incidents

SOP for handling Cybersecurity Incidents in the Securities Market

1. As per the cybersecurity and cyber resilience frameworks issued by SEBI for various market participants, cybersecurity incidents have to be reported by all MIIs and REs to SEBI in a time bound manner. It may be noted that in case any Intermediary does not report any cybersecurity incident to SEBI (when the Intermediary is aware of the incident) in a manner as laid down in the applicable cybersecurity framework, a financial disincentive/ regulatory action may be taken by SEBI as deemed fit depending on the nature of the incident.

2. Whenever an incident is reported[39] to SEBI by an Intermediary, the following steps need to be taken:

2.1. The incident shall be reported on the SEBI Incident Reporting portal by the intermediary. The incident shall also be reported to Indian Computer Emergency Response Team (CERT-In) in accordance with the guidelines/regulations/circular issued by CERT-In from time to time. Additionally, any entity whose systems have been identified as “Critical Information Infrastructure (CII)/ protected system” by National Critical Information Infrastructure Protection Centre (NCIIPC), should report the incident to NCIIPC.

2.2. The Intermediary shall undertake the necessary activities and submit the following reports as per the following timeline:

Table 1-

Sr. No.	Name of the Report / Activity	Timeline for Submission (from the date of reporting the incident or being made aware of the incident)
1	Interim Report*	3 Days
2	Mitigation measure	7 Days
3	Root Cause Analysis (RCA) report**	14 Days#
4	Forensic Audit Report (on the incident) and its closure report	Refer Below

[39] Cybersecurity incidents have to be reported by MIIs and SEBI registered intermediaries in accordance with the framework/circular/Standard Operating Procedure issued by SEBI.

5	VAPT for the incident and its closure reports	Refer Below
6	Compliance to point no 4 and 5 of Table 1	Refer Below
7	Any other report as required by SEBI	To be submitted as per direction of SEBI

*The interim report must contain, inter alia, the following: Details of the incident including time of occurrence, information regarding affected processes/ systems /network /services, severity of the incident[40], and the steps taken to initiate the process of response and recovery.

**The RCA report should inter-alia include exact cause of the incident (including root cause from vendor(s), if applicable), exact timeline and chronology of the incident, details of impacted processes/ systems /network /services, details of corrective/ preventive measures taken (or to be taken) by the entity along with timelines and any other aspect relevant to the incident. Additionally, it should also include time when operations/ functions/ services were restored and in the event of a disaster, time when disaster was declared.

# Additional time may be provided by SEBI for the submission of RCA on a case-by-case basis on the prayers of the Intermediary taking into account the complexity and nature of the incidents. The same should be an exception rather than the rule.

2.3. The RCA, forensic audit, VAPT reports, and closure reports should be reviewed by SCOT/ Technology Committee of the MII/Intermediary before the reports are submitted to SEBI. A report on the review conducted/recommendations provided by SCOT/ Technology Committee should also be submitted to SEBI along with the above mentioned reports.

2.4. On the basis of the time of submission of the interim, mitigation measure and RCA reports (along with comments/recommendations of SCOT/Internal technology committee), the following are the possible scenarios-

a. **Scenario 1:** The Intermediary submits all the reports within the stipulated timeline.

b. **Scenario 2:** The Intermediary submits some/all the reports after the stipulated timeline but within 28 days of reporting the incident.

c. **Scenario 3:** The Intermediary submits some/all the reports after 28 days of reporting the incident or the Intermediary does not submit any reports at all.

[40] Guidelines to determine the severity of the incident are given in Annexure-N

2.5. In case the reports are found to be deficient or inaccurate in any manner (for instance no identification or incorrect identification of root cause, inaccurate sequence of events, etc.), a financial disincentive may be levied on the intermediary. The intermediary shall be provided an additional time of 7 days from the day of being notified of the deficiency/ inaccuracy, for submitting the accurate and complete report.

2.6. In the event of the Intermediary not submitting accurate and complete reports after being provided additional time, a further financial disincentive may be levied on the intermediary (over and above the disincentive mentioned in clause 5 above). The matter will then be reviewed by HPSC-CS/ SEBI (whichever is applicable).

Scenario 1

i. On the basis of the reports submitted by the intermediary, the matter may be put up for the review[41] of HPSC-CS by SEBI.

Review by HPSC-CS

ii. The committee will examine the reports, review the severity of the incident[42] and provide its recommendations on the same.

iii. Further, if the committee determines that the incident occurred on account of non-compliance of SEBI cybersecurity framework/advisories, a financial disincentive may be levied by SEBI on the Intermediary notwithstanding any disincentive levied above.

iv. The recommendations of the committee must be implemented by the Intermediary in a time-bound manner. The timelines for the implementation shall be decided by the committee based on the discussion with relevant stakeholders (i.e. SEBI and the Intermediary).

v. In case the recommendations are not implemented by the Intermediary within the prescribed timeline, a financial disincentive/ regulatory action may be taken by SEBI.

Review by SEBI

i. If the matter is not put up for the review of HPSC-CS, SEBI will examine the same (on the basis of the documents submitted by the Intermediary).

[41] Incidents classified as High or Critical will be mandatorily put up for the review for HPSC-CS

[42] The committee may confirm the severity as decided by the Intermediary or may recommend a different severity on the basis of its analysis.

ii. Further, if SEBI determines that the incident occurred on account of non-compliance of SEBI cybersecurity framework/adviosries, a financial disincentive may be levied on the Intermediary notwithstanding any disincentive levied above.

iii. SEBI, after discussion with the intermediary, shall formulate a remediation and mitigation plan. The timelines for implementation of the measures shall also be decided based on the discussions (between SEBI and Intermediary). In case the measures are not implemented by the Intermediary within the prescribed timeline, Financial Disincentives/ Regulatory Action may be taken by SEBI.

Scenario 2

i. If the Intermediary submits some/all of the reports (Interim, mitigation measures and RCA, along with comments/recommendations of SCOT/Internal technology committee) after the stipulated timeline (Table 1) but within 28 days of reporting the incident, a financial disincentive may be levied on the Intermediary.

ii. After all the reports have been submitted by the Intermediary, the process established in Scenario 1 (above) will be followed.

Scenario 3

If the Intermediary submits some/all of the reports (Interim, mitigation measures and RCA, along with comments/recommendations of SCOT/Internal technology committee) after 28 days of reporting the incident or does not submit any reports at all, SEBI may initiate regulatory action against the Intermediary along with levying a financial disincentive.

3. Forensic Investigation/ Audit

3.1. For all incidents classified as High or Critical, the intermediary has to submit a forensic audit/ investigation report. Additionally, the associated closure reports should also be submitted.

3.2. For incidents classified as low or medium, forensic report should be submitted if it is required to find out the root cause or if the SEBI/ HPSC-CS directs the same.

3.3. After the completion of forensic audit, the Intermediary shall submit a final closure report, which must include the root cause of the incident, its impact and measures to prevent recurrence. The timeline for submission of the reports (including closure reports), shall be decided based on discussion with all stakeholders. However, the maximum period for the submission of forensic audit report shall be as follows:

Sr. No.	Severity of Incident	Maximum Duration for Submission of Reports
1	Low / Medium	75 Days from the Date of Incident or Intimation by SEBI
2	High / Critical	60 Days from the Date of Reporting of Incident

In case the report is not submitted by the Intermediary within the prescribed timeline, a financial disincentive/ regulatory action may be taken by SEBI.

3.4. For all the issues/ observations submitted in the forensic report, the intermediary shall provide a timeline for fixing the same. This timeline should be submitted along with the forensic investigation/ audit report. Once the issues are resolved, the intermediary shall file a closure report for the same.

3.5. In case the issues are not fixed within the prescribed timeline, a financial disincentive/ regulatory action may be taken by SEBI.

Annexure-P: Recovery Plan Template

Recovery plan Template for the REs

1	Cybersecurity incident recovery plan	i. Preparation: Measures taken in preparation for cybersecurity incident (pre-incident).	
		ii. Identification Checklist	a. Who has discovered or reported the incident?
			b. When it is discovered?
			c. What is discovered?
			d. What is the location of the incident?
			e. The impact of the incident on the business operations
			f. What is the extent of the incident with applications and networks?
		iii. Containment checklist	a. Can the incident be isolated? 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. Has 'golden' server images and data identified?
			d. Does latest data backup as per prescribed RPO available?
			e. Has copy of the infected machines to preserve for digital forensics and incident response experts for analysis?
			f. Has the threat been removed from the infected devices?
		iv. Eradication checklist	Eradicating the cause of the incident by removing malware, patching vulnerabilities, and taking other measures.

		v. Recovery checklist	Recover lost or corrupted data and restore normal operations by returning systems and networks to a known good state.
2	Cybersecurity incident recovery plan scenarios		
3	Categorization of incidents		
4	Key assumptions and pre-requisites		
5	Authorization		
6	Incident Response Team (IRT)		
7	Other teams involved		
8	Cybersecurity incident recovery invocation		
9	Off site location address where ‘golden’ copy of server image and data is 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 repetition of the cyber incident		
14	Perform Hotwash		