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:

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

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 organization 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		