AN ASSOCIATION FOR THE COMMUNITY OF PORTFOLIO MANAGERS REGISTERED WITH THE SECURITIES & EXCHANGE BOARD OF INDIA

Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs)

The Securities and Exchange Board of India (SEBI) with industry feedback and its commitment to creating a robust, flexible, and comprehensive cyber security framework issued the CSCRF for all the REs .The frameworks gives the detailed understanding of the diverse needs of REs, the complex nature of cyber threats, and the importance of operational resilience in the financial sector.

By balancing prescriptive requirements with risk-based approaches, SEBI has crafted a framework that aims to enhance the overall cyber security posture of India's securities market while allowing for the operational realities of diverse market participants.

This guidance highlights the regulator's proactive stance in enhancing the Cybersecurity and Resilience of its regulated entities, ensuring they are not only compliant but also well-equipped to handle the complexities of modern cyber threats.

The Framework lays the guidelines to controls and protect Asset Managers information, systems, databases and networks from emerging cyber threats while ensuring Confidentiality, Integrity and Availability (CIA).

Thresholds for REs' categorization

CSCRF follows a graded approach and classifies the REs in the following categories based on Span of operations and certain thresholds like;

- Number of Clients
- Trade Volume
- **Asset Under Management**

Categorization

- Market Infrastructure Institutions (MIIs)
- Qualified REs
- Mid-size REs
- Small-size REs
- Self-certification REs

CSCRF framework provides a structured methodology to implement various solutions for cybersecurity and cyber resiliency.

In case an RE is registered under more than one category, then the provision of **highest category** under which such an RE falls **shall be applicable**.

Categorization for PMS

The category of REs shall be decided at **the beginning of the financial year** based on the data of the previous financial year.

Once the category of RE is decided, RE shall remain in the same category throughout the financial year irrespective of any changes in the parameters during the financial year.

Criteria (PMS)	Self- certification REs	Small-size REs	Mid-size REs
AUM	Less than Rs. 1000 crores	Rs. 1000 crores and above but less than Rs. 3000 crores	Rs.3000 crores and above

Goals

CSCRF is based on five Cyber Resiliency goals namely Anticipate, Withstand, Contain, Recover, and Evolve.

ANTICIPATE: Maintain a state of informed preparedness in order to forestall compromises of mission/ business functions from adversary attacks.

WITHSTAND: Continue essential mission/business functions despite successful execution of an attack by an adversary.

CONTAIN: Localize containment of crisis and isolate trusted systems from untrusted systems to continue essential business operations in the event of cyber-attacks.

RECOVER :Restore mission/ business functions to the maximum extent possible, subsequent to successful execution of an attack by an adversary.

EVOLVE: To change mission/ business functions and/or the supporting cyber capabilities, so as to minimize adverse impacts from actual or predicted adversary attacks

The framework is broadly based on two approaches: cybersecurity and cyber resilience.

Cybersecurity – Covers Governance to operational controls (including Identify, Detect, Protect, Respond, and Recover) and the cyber resilience goals include Anticipate, Withstand, Contain, Recover, and Evolve.

Guidelines - Applicability

Particulars	Self-Certified RE'S	SMALL SIZE RE'S	MID SIZE RE'S
Implementation of Cybersecurity Policy	✓ **(Basic Policy Covering essential areas)**	✓ (Basic policy covering essential areas)	✓ (Detailed policy, To be updated annually)
Risk Management	✓ **(Basic Risk Assessment)**	✓ (Conduct risk assessments Annually)	✓ (Conduct periodic risk assessments and scenario-based testing)
List of Critical Assets - Software **Software Bill Of Material (SBOM)**	✓	✓	✓

Guidelines - Applicability

Particulars	Self-Certified RE'S	SMALL SIZE RE'S	MID SIZE RE'S
Conduction of Cyber Security Training	✓ (Annually)	✓ (Basic Cybersecurity Training Annually)	✓ (Cybersecurity Training Semi-Annually)
Conduct Vulnerability Assessment and Penetration Testing (VAPT)	✓ (Annually)	✓ (Annually)	✓ (Annually)
Cyber Audits	✓ (Annually) **Self Certification (Annexure-P)**	✓ (Annually)	✓ (Annually)
ISO and other Compliances	✓ **(Best Practices to be adopted)**	✓ (SEBI guidelines and ISO 27001 standards)	✓ (SEBI guidelines and ISO 27001 standards)
Security Operations Center (SOC) – Functional Efficacy	✓	✓ (Continuous Monitoring)	✓ (Continuous Monitoring)

Guidelines - Applicability

Particulars	Self-Certified RE'S	SMALL SIZE RE'S	MID SIZE RE'S
User Credentials – Complexity and processes	✓	✓	✓
Physical Access Remote Support – Stringent Monitoring	✓	✓	✓
Data Availability And Classification Need based Access Data Protection /Backup Recovery	✓	✓	✓
Secure Infra Design	✓	✓	✓

Guidelines - Applicability

Particulars	Self-Certified RE'S	SMALL SIZE RE'S	MID SIZE RE'S
Patch Management , EOL,MECHANISM, Tech Refresh	✓	✓	✓
Incident Management /CCMP	✓ **(In line with Cert-In)**	✓ (Develop and review Incident Response Plan annually)	✓ (Maintain a comprehensive Incident Response Plan)
Incident Reporting	✓ (Within 24 hours of detection on SEBI Portal)	✓ (Within 24 hours of detection on SEBI Portal)	✓ (Within 24 hours of detection on SEBI Portal)
Appointment Qualified CISO	Designated Personnel or Management Personnel	Designated Personnel or Management Personnel	Designated Personnel
IT Committee	Not Mandatory	Not Mandatory	✓ (Mandatory – IT Committee' must include at least one (01) external independent Technology Expert.)

Guidelines - Applicability

Particulars	Self-Certified RE'S	SMALL SIZE RE'S	MID SIZE RE'S
IT Budget Allocation	Not Mandatory	Not Mandatory	✓
Network Segmentation	Not Mandatory	Not Mandatory	✓
AD Management and Controls Including STRONG Password control mechanism	Not Mandatory	Not Mandatory	✓
Employee Due Diligence, screening and Training	Not Mandatory	Not Mandatory	✓
Third Party – Vendor Due Diligence /Agreement	Not Mandatory	Not Mandatory	✓

Guidelines - Applicability

Particulars	Self-Certified RE'S	SMALL SIZE RE'S	MID SIZE RE'S
PIM/PAM Solution	Not Mandatory	Not Mandatory	✓
Internet Access Policy **Network Segmentation** **SPF/DMARC/DKIM/DNS filtering**	Not Mandatory	Not Mandatory	✓
AD management and Controls	Not Mandatory	Not Mandatory	✓
DLP solution /Appropriate Data Usage Policy	Not Mandatory	Not Mandatory	✓
Capacity Planning and Monitoring	Not Mandatory	Not Mandatory	✓
Continuous evolving /learning - Anticipate through Threat modelling/threat reduction through learning	Not Mandatory	Not Mandatory	✓

Compliance, Audit Report Submission, and Timelines

APMI ASSOCIATION OF PORTFOLIO MANAGERS IN INDIA

Standard/ Guidelines and Clause	Self - Certified REs	Small-Size REs	Medium-Size REs
Cybersecurity and cyber resilience policy review	Annually	Annually	Annually
Cybersecurity risk management policy	Annually	Annually	Annually
Cybersecurity training program	Annually	Annually	Annually
Review of RE's systems managed by third-party service providers	Annually	Annually	Annually
Functional Efficacy of SOC	Annually	Annually	Annually
Cybersecurity scenario-based drill exercise for testing adequacy and effectiveness of recovery plan	Annually	Annually	Annually
VAPT Activity	Annually	Annually	Annually

Compliance, Audit Report Submission, and Timelines

Standard/ Guidelines and Clause	Self - Certified REs	Small-Size REs	Medium-Size REs
Cyber Audit	Self Certified –as per Format	Annually	Annually
Review of periodically and update their contingency plan, continuity of operations plan	-	Annually	Annually
Evaluation of cyber resilience posture	-	Annually	Annually
Review of periodically and update their contingency plan, continuity of operations plan	-	Annually	Annually
Evaluation of cyber resilience posture	-	Annually	Annually
REs' risk assessment	-	-	Annually
User access rights, delegated access and unused tokens review	Half Yearly	Half Yearly	Half Yearly

Compliance, Audit Report Submission, and Timelines

Standard/ Guidelines and Clause	Self - Certified REs	Small-Size REs	Medium-Size REs
Review of privileged users' activities	Half Yearly	Half Yearly	Half Yearly
IT Committee for REs meeting periodicity	-	-	Quarterly
Cyber resilience self-assessment using CCI (GV.OV.S4)	-	-	-
Submission of CCI self-assessment evidence	-	-	-
Red Teaming exercise	-	-	-
Threat hunting	-	-	-

NOTES:

- In the absence of IT Committee for REs for Small-size REs and Self- certification REs, the compliance to CSCRF shall be reviewed and approved by MD/ CEO/ Board member/ Partners/ Proprietor.

- Incident Reporting shall be shared to SEBI on **mkt_incidents@sebi.gov.in** within 6 hours and SEBI Incident Reporting Portal within 24 hours.

- **Cert-In - Cyber Crisis Management Plan;**

(https://www.cert-in.org.in/Downloader?pageid=5&type=2&fileName=CIPS-2017-0121.pdf)

VAPT – Periodicity and Report Submission

- Vulnerability Assessment & Penetration Testing (VAPT) must be conducted by the REs on periodic basis
- The Scope & Compliance is as provided in the standard DE.CM.S5 and the corresponding guidelines.
- The REs have to submit the VAPT report along with a Declaration signed by MD/CEO as per the format provided by SEBI in Annexure – A of the Circular to SEBI.
- VAPT must be carried out **Annually** and must be **commenced at the beginning** of the financial year
- REs shall ensure that no audit cycle shall be left unaudited (if any) due to the change in category.
- In case, any period is left unaudited then the same shall be included in the current cycle of the audit.
- The Timeline for VAPT activity is as follows:

Activity	Format	Periodicity	Timelines	Reporting to
Conduct VAPT Activity	Scope as specified by SEBI	Annually	VAPT activity shall commence in the first quarter of the financial year	SEBI
Report submission of VAPT and Declaration by MD/CEO	As per the format provided by SEBI	Annually	Within 1 month of Completion of VAPT	SEBI
Closure of findings identified during VAPT activity	-	Annually	Within 3 months of submission of VAPT report	SEBI
Revalidation of VAPT	-	Annually	within 5 months of completion of VAPT	SEBI

Any open vulnerabilities after 3 months of VAPT activity shall be approved by IT Committee for REs and shall be closed before start of next VAPT exercise.

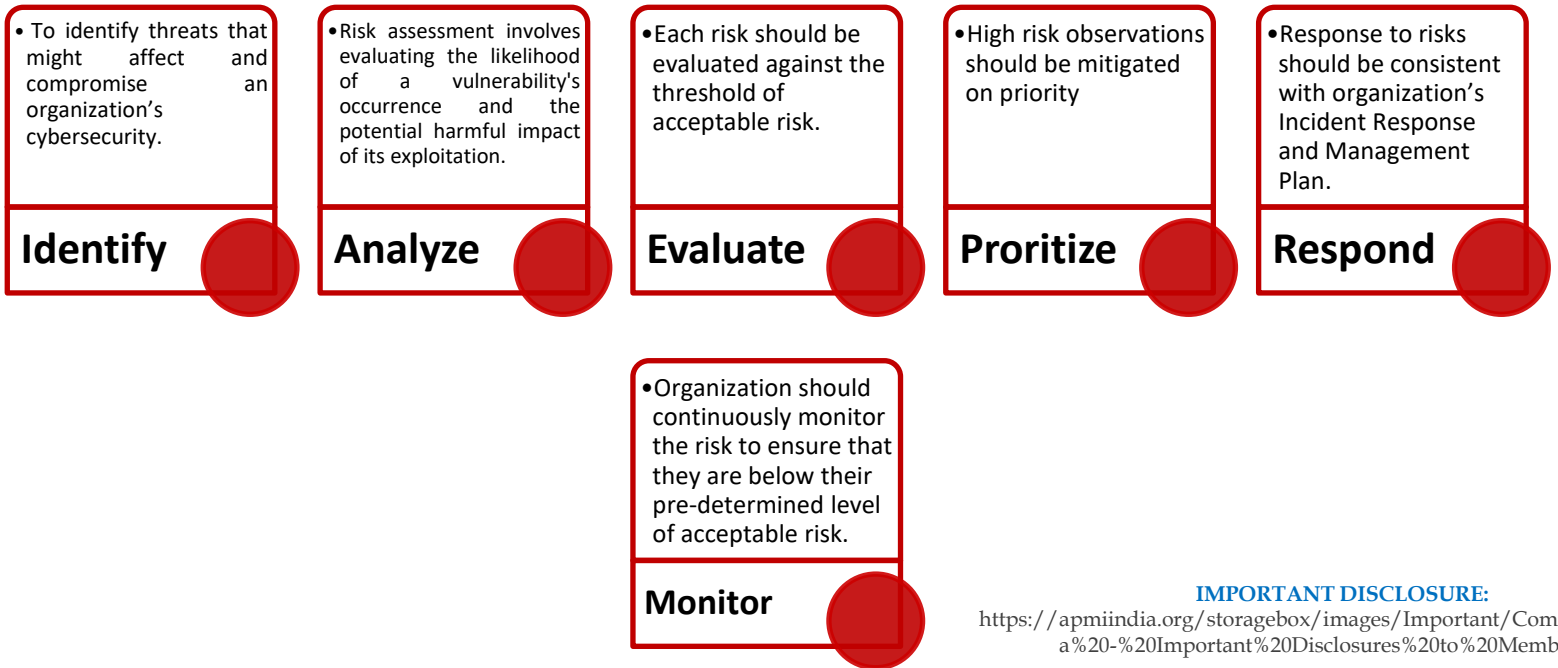
Cyber Audit Periodicity and Submission

- Cyber audit here pertains to the audit conducted for verifying the compliance with CSCRF and the report of the same and a declaration from MD/CEO must be submitted with SEBI as per the format prescribed in Annexure-B of the circular.
- Cyber Audit to be carried out by CERT-In empanelled IS auditing organization and the guidelines of the same is as provided by SEBI.
- REs shall ensure that no audit cycle shall be left unaudited (if any) due to the change in category in the beginning of the financial year.
- **Cyber Audit is not applicable for Self-certification RE. They have to submit a compliance report as per Annexure-P of the circular signed by the MD/CEO/Board Member/Partners/Proprietor.**
- The Timelines for Cyber Audit is as follows:

Activity	Format	Periodicity	Timelines	Reporting to
Conduct Cyber Audit	Scope as spcified by SEBI	Yearly/Half-Yearly		SEBI
Submission of Cyber Audit Report and a Declaration by MD/CEO	As per the format provided by SEBI	Yearly/Half-Yearly	within 1 month of completion of cyber audit.	SEBI
Closure of findings identified during cyber audit	-	Yearly/Half-Yearly	Within 3 months of cyber audit report submission	SEBI
Follow-on audit	-	Yearly/Half-Yearly	within 5 months of completion of cyber audit.	SEBI

Cyber Risk Management Framework

- Cyber risk management enables an organization to identify, prioritize, manage and monitor risks to their IT/ information systems and infrastructure.
- Cyber risk management is a continuous and iterative process that necessitates continuous improvement and assessment of security controls by incorporating emerging new information and responding to latest threat landscape. Cyber risk management includes:



Adoption

- PMS entities with AUM more than INR 3000 Crs where cybersecurity and cyber resilience circular already exists- January 01, 2025

- All other PMS entities for AUM less than INR 3000 Crs.– April 01, 2025

THANK YOU

1. ***The information provided herein is for general purpose only and should not be construed as a guidance or legal opinion from APMI.***
2. ***APMI shall not be responsible for any views / opinion / guidance / advice given above.***
3. ***The members are expected to do their own due diligence before acting on the advice or guidance given and seek independent legal / expert advice when in doubt.***
4. ***APMI will not be in any manner responsible for any loss incurred by, or damage caused to, the member(s) for their action based on the information provided by the APMI to its member(s).***

IMPORTANT DISCLOSURE:

https://apmiindia.org/storagebox/images/Important/Compliance%20Sutra%20-%20Important%20Disclosures%20to%20Members.pdf