भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

परिपत्र / CIRCULAR

SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2025/119 ***August 28, 2025***

To,

All Alternative Investment Funds (AIFs)

All Bankers to an Issue (BTI) and Self-Certified Syndicate Banks (SCSBs)

All Clearing Corporations

All Collective Investment Schemes (CIS)

All Credit Rating Agencies (CRAs)

All Custodians

All Debenture Trustees (DTs)

All Depositories

All Designated Depository Participants (DDPs)

All Depository Participants through Depositories

All Investment Advisors (IAs) / Research Analysts (RAs)

All KYC Registration Agencies (KRAs)

All Merchant Bankers (MBs)

All Mutual Funds (MFs)/ Asset Management Companies (AMCs)

All Portfolio Managers

Association of Portfolio Managers in India (APMI)

All Registrar to an Issue and Share Transfer Agents (RTAs)

All Stock Brokers through Exchanges

All Stock Exchanges

All Venture Capital Funds (VCFs)

BSE Limited (Investment Adviser Administration and supervisory body- IAASB)

BSE Limited (Research Analysts Administration and supervisory body- RAASB)

Sir / Madam,

Subject: <u>Technical Clarifications to Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs)</u>

1. Recognising the need for robust cybersecurity measures and protection of data and IT infrastructure, Securities and Exchange Board of India (SEBI) has issued '*Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs)*' vide circular *SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113* dated August 20, 2024.

2. Upon receipt of various queries from REs seeking extension and clarification on the aforementioned circular, SEBI has also issued following clarifications and Frequently Asked Questions (FAQs):

S. No.	Circular Title	Circular Number	Date of Issuance
1.	Clarifications to Cybersecurity and Cyber Resilience Framework (CSCRF)for SEBI Regulated Entities (REs)	SEBI/HO/ITD-1/ ITD_CSC_EXT/ P/CIR/2024/184	December 31, 2024
2.	Extension towards Adoption and Implementation of Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs)	SEBI/HO/ITD-1/ ITD_CSC_EXT/ P/CIR/2025/45	March 28, 2025
3.	Clarifications to Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs)	SEBI/HO/ITD-1/ ITD_CSC_EXT/P/ CIR/2025/60	April 30, 2025
4.	Frequently Asked Questions (FAQs) on Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI REs and Framework for	FAQs	June 11, 2025

S. No.	Circular Title	Circular Number	Date of Issuance
	Adoption of Cloud Services by SEBI REs		
5.	Extension towards Adoption and Implementation of Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs)	SEBI/HO/ITD-1/ ITD_CSC_EXT/P/ CIR/2025/96	June 30, 2025

3. Based on further discussions, technical clarifications are being issued with respect to Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs) in following parts:
   3.1. Part-A: Principles for REs under multiple regulators' purview
   3.2. Part-B: Technical clarifications
   3.3. Part-C: Re-categorisation of Portfolio Managers and Merchant Bankers
   3.4. Part-D: Cyber Security Audit Policy Guidelines from CERT-In

Part – A: Principles for SEBI REs under multiple regulators' purview

4. There are several SEBI REs engaged in various business operations, and their activities are being regulated by multiple regulatory bodies within the Indian jurisdiction. For example: SEBI REs such as Custodians, Depository Participants (DPs) Merchant Bankers (MBs), etc. are also banks which are being primarily regulated by Reserve Bank of India (RBI).
5. Following clarifications are being issued for such REs w.r.t. CSCRF issued vide SEBI circular *SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113* dated August 20, 2024:
   5.1. There are various standards and corresponding guidelines mentioned in CSCRF which REs need to implement and comply with in a certain manner. For the ease of compliance and clarity of implementation, following *Principle of Exclusivity* and *Principle of Equivalence* have been formulated. During submission of CSCRF compliance, REs need to demonstrate that they follow

the principle of equivalence and/ or exclusivity for the applicable controls. Further, SEBI reserves the right to seek the submissions made by the REs to other regulators to verify their compliances.

5.2. **Principle of Exclusivity:** The scope of CSCRF shall be limited to only those systems/ applications/ infrastructure/ processes which are exclusively used for SEBI regulated activities. Further, the shared infrastructure/ network/ technology stack, security solutions shall be included in the audit/ inspection scope by SEBI, if the same is not covered under audit/ inspection scope by primary regulator and their frameworks/ guidelines.

Following are representative examples of the standards and corresponding guidelines as mentioned in CSCRF:

Table 1: Representatives examples under *Principle of Exclusivity*

S. No.	CSCRF Standard/ Guidelines	CSCRF Clause
1.	Data Classification (Regulatory Data, and IT and Cybersecurity Data) and Data Localisation (currently in abeyance vide SEBI circular *SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/184* dated December 31, 2024)	Box Item 9, Box Item 10, and PR.DS.S1-3 Guidelines (Page 107)
2.	Definition and classification of Critical/ non-critical systems	Definitions (Page 26), ID.AM.S1 and ID.AM.S4 Guidelines (Page 90)
3.	VAPT scope	Scope given in Annexure-A (Page 136), Annexure-L, and DE.CM.S5 Guideline 2 (Page 120)
4.	Asset inventory updation timelines	ID.AM.S1 and ID.AM.S4 Guidelines 3 (Page 90)

S. No.	CSCRF Standard/ Guidelines	CSCRF Clause
5.	Patch management timelines	PR.MA.S3 Guidelines 11 (Page 117-118)
6.	SEBI Cloud circular compliance	Annexure-J
7.	Supply chain risk management	GV.SC and corresponding guidelines
8.	Requirements of log management and retention	PR.AA.S8-9 and corresponding Guideline (e) (Page 93)

5.3. **Principle of Equivalence:** CSCRF controls which have an equivalence in other regulators' cybersecurity frameworks/ guidelines shall be deemed compliant provided that the frameworks/ guidelines issued by primary regulator are adhered by such REs.

Following are representative examples of the standards and corresponding guidelines as mentioned in CSCRF:

Table 2: Representatives examples under *Principle of Equivalence*

S. No.	CSCRF Standard/ Guidelines	CSCRF Clause
1.	Cyber Capability Index (CCI)	GV.OV.S4, corresponding guidelines and Annexure-K
2.	IT Committee constitution with an external independent cybersecurity expert or an independent director having IT and cybersecurity expertise, and various approval required from them	Clause 3.3-3.5 of Section 3 – IT Committee for REs (Page 44)
3.	Patch Management policy	PR.MA.S3 Guidelines 8-10 (Page 117-118)
4.	Cybersecurity policy	GV.PO.S1-4 (Page 54) and corresponding guidelines (Page 82-83)

S. No.	CSCRF Standard/ Guidelines	CSCRF Clause
5.	Requirement of having Information Technology Service Management (ITSM) tool for managing asset inventory	ID.AM.S6 and corresponding guidelines (Page 91)
6.	Red Teaming Exercise and requirement of placing report before IT committee	DE.DP.S4 and corresponding guidelines 1-4
7.	SOC efficacy	Annexure-N, DE.CM.S3 Guideline 2-3 (Page 118-119)

Part – B: Technical clarifications

6. Technical Clarification for the following CSCRF clauses are given below:

6.1. Critical Systems definition (Page 26)*: 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, if compromised, that will have an adverse impact on core and critical business operations.*
b. *Stores/ transmits data as per regulatory requirements.*
c. *Devices/ network through which critical systems are connected (through trusted channels).*
d. *Internet facing applications/ systems.*
e. *Client facing application/ systems.*
f. *All the ancillary systems used for accessing/ communicating with critical systems either for operations or for maintenance."*

Clarification: Above-mentioned para (f) shall now be read as under: Any other system which is on the same network segment where systems mentioned in para (a) to (e) are deployed.

6.2. Zero-trust security model (PR.AA.S4 and PR.AA.S5 guidelines – Page 97): *"REs shall follow zero-trust security model in such a way that access (from within or outside REs' network) to their critical systems is denied by default and allowed only after proper authentication and authorization."*

Clarification: Above-mentioned guidelines shall now be read as under: REs shall implement suggested strategies/ methodologies such as Zero-trust networks, segmentation, no single point of failure, high availability, etc. Further, the same shall be approved by *IT committee for REs*.

6.3. Mobile Application Security guidelines (PR.AA.S16 and corresponding guidelines – Page 102-103)

Clarification: Above-mentioned guidelines are recommendatory (not mandatory) in nature.

6.4. RS.CO.S2 guidelines (Page 124-125): *"If the cyber-attack is of high impact and has a broad reach, the RE shall give a press release which shall include (but not limited to) a brief of the incident, actions taken to recover, normal operation resumption status (once achieved), etc. and inform all the affected customers/ stakeholders. If the cyber-attack is of low impact and has a narrow/low reach, the REs shall inform all the affected customers/ stakeholders."*

Clarification: Above-mentioned guidelines shall now be read as under: REs shall take action as per their approved Cyber Crisis Management Plan (CCMP).

6.5. DE.CM.S3 guidelines (3.c) (Page 119): *"REs shall deploy solutions such as BAS, CART, decoy, vulnerability management, etc. to enhance their cybersecurity posture."*

Clarification: Above-mentioned guideline shall now be read as under: It is recommended that REs consider deploying a range of security solutions in consultation with their *IT Committee*, such as threat simulation, vulnerability management, and decoy systems, to assess and enhance their cybersecurity posture.

6.6. GV.SC.S2 (Page 56): *"Suppliers and third-party service providers of information systems, components, and services shall be identified, prioritized, and assessed using a cyber-supply chain risk assessment process."*

Clarification: The above-mentioned cyber-supply chain risk assessment process may be done by the REs in consultation with their IT committee.

6.7. Submission of VAPT and Cyber audit report (Section 4.3-4.4 - Page 48-52, Annexure-A, Annexure-B)

Clarification: REs shall submit the summary of VAPT and cyber audit reports strictly as per the format mentioned in CSCRF. It is clarified that at no point of time, REs shall submit the explicit vulnerabilities unless and otherwise asked for the details by SEBI.

6.8. GV.PO – Guideline 11 (Page 85): *"The cybersecurity policy shall encompass the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organisation (NTRO), GoI in the report titled 'Guidelines for Protection of National Critical Information Infrastructure' and subsequent revisions, if any, from time to time."*

Clarification: The above-mentioned clause is applicable only on REs which have been identified as Critical Information Infrastructure (CII) by NCIIPC.

6.9. On boarding to Market-SOC (Box Item 11)

Clarification: small-size and self-certification with few exclusions as mentioned in (CSCRF Box Item 11, DE.CM.S3 Guidelines (c-d) – Page 118) and (Clause 2.2, 2.6, 2.7 and 3 of SEBI circular vide *SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2025/60* dated April 30, 2025) have been mandated to be on boarded on Market-SOC. Please refer Q. 60 of CSCRF FAQs[1] issued vide dated June 11, 2025:

Question: In a scenario where an RE falling under small-size or self-certification REs category has its own SOC, is it necessary for such REs to get onboarded to Market-SOC?

Answer: It is imperative that setting up own SOC is a costly proposition. Hence, SEBI has mandated NSE and BSE to setup Market-SOC (M-SOC) where small-size REs and self-certification REs can get onboarded and take the benefit to stay cyber secure and resilient. However, REs who have their own SOC and falling under the category of small-size REs or self-certification REs by virtue of their regulatory activity may leverage their existing SOC. Further, such REs shall be required to submit the SOC efficacy report

[1] Refer https://www.sebi.gov.in/sebi_data/faqfiles/jun-2025/1749647139924.pdf

periodically as mandated in CSCRF.

6.10. RC.RP.S2 guideline (Page 128-129): *"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' based on the business impact analysis. Accordingly, the RTO shall be two (2) hours as recommended by IOSCO[2] for the resumption of critical operations. 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."*

Clarification: Above-mentioned guideline shall now be read as under as referred from IOSCO[3]: Resumption within two hours (i.e. two-hour RTO). REs shall design and test its systems and processes to enable the safe resumption of critical operations within two hours of a disruption, even in the case of extreme but plausible scenarios. Notwithstanding this capability to resume critical operations within two hours, when dealing with a disruption REs shall exercise judgment in effecting resumption so that risks to itself or its ecosystem do not thereby escalate. In consultation with their *IT Committee*, REs shall also plan for scenarios in which the resumption objective is not achieved.

Further, RPO for critical systems shall be 15 minutes as per SEBI circular[4] dated March 22, 2021.

6.11. Requirement of ISO 27001 certification for Qualified REs (PR.IP.S16 (Page 66) and corresponding guideline (Page 115), and Section 4.2 - Page 47)

Clarification: Qualified REs are encouraged and recommended (not mandatory) to obtain ISO 27001 certification.

6.12. While receiving and handling cyber audit reports submitted by their members, Stock Exchanges and Depositories shall ensure that adequate safeguards are in place to maintain the confidentiality and integrity of such reports.

[2] Refer https://www.bis.org/cpmi/publ/d146.pdf.
[3] Refer https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf
[4] Refer https://www.sebi.gov.in/legal/circulars/mar-2021/guidelines-for-business-continuity-plan-bcp-and-disaster-recovery-dr-of-market-infrastructure-institutions-miis-_49601.html

Part – C: Re-categorisation of Portfolio Managers and Merchant Bankers (MBs)

7. Based on further discussions, it has been decided to revise the thresholds and categorization of following REs as under:

7.1. Portfolio Managers

Table 1: Criteria and thresholds for Portfolio Managers categorization

S. No.	Criteria	Qualified REs	Mid-size REs	Small-size REs	Self-certification REs
1.	Asset Under Management (AUM)	N.A.	Rs. 10,000 crores and above	More than Rs. 3000 Crores and less than Rs. 10,000 Crores	Rs. 3000 Crores and below

7.2. Merchant Bankers (MBs)

Table 2: Criteria and thresholds for MBs categorization

S. No.	Criteria	Merchant Bankers (MBs) categorisation for CSCRF
1.	All active Merchant Bankers (i.e., who have undertaken any merchant banking activity during the relevant period)	Small-size REs
2.	All inactive Merchant Bankers (i.e., those have not undertaken any merchant banking activities in the relevant review period.	Exempt from CSCRF

Part – D: Cyber Security Audit Policy Guidelines from CERT-In

8. CERT-In has issued comprehensive Cyber Security Audit Policy Guidelines[5]. These guidelines are intended to serve as a reference both CERT-In empanelled auditing organisations and auditee organisations. REs shall follow these guidelines to ensure a consistent, effective and secure approach to cyber security audits.

[5] https://www.cert-in.org.in/PDF/Comprehensive_Cyber_Security_Audit_Policy_Guidelines.pdf

9. Stock Exchanges/ Depositories are directed to:
   9.1. Make necessary amendments to the relevant byelaws, rules and regulations for the implementation of the above direction and
   9.2. Bring the provisions of this circulars to the notice of their members/ participants and also disseminate the same on their websites.

10. BSE Limited is directed to:
   10.1. Make necessary amendments to the relevant byelaws, rules and regulations for the implementation of the above direction and
   10.2. Bring the provisions of this circulars to the notice of Investment Advisers (IAs) and Research Analysts (RAs) and also disseminate the same on their websites.

11. The provisions of this Circular shall come into force with immediate effect.

12. This circular is being issued in exercise of powers conferred under Section 11 (1) of the Securities and Exchange of India Act, 1992, to protect the interests of investors in securities and to promote the development of, and to regulate the securities market.

13. This circular is issued with the approval of Competent Authority.

14. This circular is available on SEBI website at www.sebi.gov.in under the category “Legal” and drop “Circulars”.

भवदीय / Yours faithfully,
मृदुस्मिता गोस्वामी / Mridusmita Goswami
मुख्य सूचना सुरक्षा अधिकारी - महाप्रबंधक / CISO - General Manager
दूरभाष / Phone: 022-26449504
ईमेल / Email: mridusmitag@sebi.gov.in