HELP DOCUMENT ON SEBI CSCRF CIRCULAR DATED AUGUST 20, 2024

Over the past 10–12 months, APMI has conducted numerous sessions and shared multiple communications with its Members and Industry participants on the compliances, execution, and implementation of the SEBI CSCRF Circular dated August 20, 2024.

As we approach the implementation date, by this document we have consolidated all related communications and included a set of relevant questions specifically curated for Self-Certified RE's- Who constitute a significant segment of the PMS industry.

This document covers the details under **3 important aspects** for a Self-Certified RE:

Sr. No.	Particulars
A	**Questions of a Self-Certified RE regarding CSCRF**
B	**Important Points & Activities to be Completed**
C	**Communication Archive**
D	**Disclosures**

A. Questions of a Self-Certified RE regarding CSCRF:

1. **Are we exempted from conducting a Cyber Audit?**

   Yes, Cyber Audit by an external CERT-IN empanelled auditor is exempted for Self-Certified PMS.

   However:

   - VAPT (Vulnerability Assessment and Penetration Testing) is mandatory (at least annually).
   - Internal audits are not explicitly mandated under CSCRF for Self-Certified entities, but:
   - If your organization performs internal IT/cyber reviews, it's advisable to document them.
   - Having an internal cyber review mechanism (even if lightweight) adds strength to your compliance.
   - Audit Policy: While a full-fledged policy may not be mandatory, it's recommended to mention internal review practices in your main CSCRF policy document.

2. **Given M-SOC exemption, do Self-Certified entities require a SOC or SOC policy at all?**

   As per the latest SEBI clarification, Self-Certified entities are exempted from M-SOC onboarding only if they have less than 100 clients/investors.

Implications:

- Setting up your own SOC or subscribing to third-party SOC is not mandatory.
- However, basic log retention, incident monitoring and alert handling should be covered within the CSCRF policy, even without SOC.

3. **Is the full APMI policy suite mandatory for Self-Certified entities with <100 clients? Can one comprehensive CSCRF policy suffice?**

A total of 14 policy templates have been made available to APMI Members.

- These are standard reference documents.
- Portfolio Managers may customize them to align with their specific IT infrastructure and operational requirements.

4. **Is Patch Management applicable to Self-Certified organizations?**

Yes, Patch Management (including testing before deployment) is applicable to all entities, including Self-Certified.

However:

- The scale and documentation of patch testing can be proportionate to your operations.
- A simple process note for testing updates on non-production systems (or during low-usage hours) is acceptable.

5. **Are Real-Time Simulation (RTS) tests required for the Self-Certified category?**

No, Real-Time Simulation (RTS) or Red Teaming exercises are not mandatory for Self-Certified entities.

However:

- You must conduct VAPT annually.
- It is also recommended (not mandated) to conduct Tabletop exercises or DR simulations internally.

6. **What is the reporting frequency to SEBI for CSCRF compliance for Self-Certified entities- Annual or Quarterly?**

As per clarifications:

- Self-Certified entities must submit an annual self-declaration of CSCRF compliance to SEBI.
- No quarterly reporting is required for Self-Certified entities.

- The annual compliance self-declaration should be submitted within 30 days of the end of the financial year.

7. Is a Business Continuity Plan (BCP) necessary for Self-Certified REs?

Yes, a basic but well-defined BCP is expected, even for entities under the Self-Certified category.
The plan should outline key contact persons, backup protocols, access restoration processes, and continuity arrangements in case of disruption. While a full-scale DR site is not mandated, a documented fallback mechanism should be in place.

8. Is a specific allocation for cybersecurity budgets or resourcing required?

There is no regulatory mandate to maintain a dedicated cybersecurity budget. However, entities are expected to demonstrate reasonable allocation of resources towards essential cybersecurity functions—such as VAPT, log management, endpoint protection, and incident handling—based on their operational scale.

9. Can IT infrastructure be entirely outsourced to third parties?

Yes, Self-Certified REs may fully outsource IT infrastructure to external service providers including cloud platforms or managed IT partners. However, the regulatory responsibility continues to rest with the RE. Contracts must include appropriate provisions related to data protection, breach notification, and access to logs. A vendor register along with service-level documentation, should be maintained.

10. Is data encryption required for Self-Certified REs?

- Encryption during data transmission (e.g., using HTTPS or email encryption) is expected as a minimum standard.
- While encryption of data at rest is not explicitly required for Self-Certified entities, it is advisable to implement it wherever feasible.

11. What cybersecurity controls apply during employee offboarding?

- Entities must ensure immediate revocation of access upon employee exit.
- This should include disabling user credentials, re-cover all issued IT assets, and revoke any active authentication tokens.
- A clear offboarding protocol should be documented, and a log of such activities maintained for accountability.

12. Are digital onboarding processes covered under the CSCRF framework?

- Yes. If the onboarding process involves sensitive personal or financial data, it must be secured and fall under the scope of CSCRF. Authentication mechanisms (e.g., OTP, eSign, Aadhaar verification) should be documented, and all systems involved in digital onboarding must implement baseline cybersecurity measures.

13. Can Self-Certified entities adopt a unified CSCRF policy instead of multiple documents?

A total of 14 policy templates have been made available to APMI Members.

1. These are standard reference documents.
2. Portfolio Managers may customize them to align with their specific IT infrastructure and operational requirements.

14. Is cybersecurity training necessary for small teams?

Yes, annual cybersecurity awareness training is mandatory irrespective of team size. For smaller teams, a simplified format—such as an internal session or recorded briefing is acceptable. Attendance should be tracked, and the training agenda retained for reference.

15. Are cybersecurity dashboards or formal metrics reporting required?

No, real-time dashboards are not required for Self-Certified REs. However, entities must keep a basic record of cybersecurity activities such as VAPT reports, access reviews, and incident logs. These should be summarized and submitted as part of the annual CSCRF self-declaration to SEBI.

B. Important Points & Activities to be Completed:

1. Cybersecurity Policy & Governance

- Draft and adopt a Cybersecurity Policy aligned to CSCRF requirements.
- Review and approve the Policies by Designated Partners / Board
- Pass a Resolution to approve the Policies before **June 30, 2025**.

2. Appointment of Designated CISO

- Individuals identified as designated CISO from Group-level CISO or internal senior personnel.
- Pass a Resolution for appointment and alongside policy approval.

3. Endpoint Security Mitigations

- Complete the Gap Assessment.
- Identify the gaps in Windows licensing, antivirus/EDR, and MS Office versions.
- Initiate the evaluation of the EDR solutions.

4. **Vulnerability Assessment and Penetration Testing (VAPT)**

   - Initiate VAPT.
   - Closure and submission of final (ATR) report by July 31, 2025, as per the format provided in the CSCRF Circular.
   - Submit via email on **vapt_reports@sebi.gov.in.**

C. Communication Archive:

1. **CSCRF Circular- SEBI- 20th August'24:**
   - https://www.apmiindia.org/storagebox/images/Important/Circular%20-%20CSCRF%20-%2020th%20Aug'24.pdf

2. **Update on CSCRF Circular by APMI:**
   - https://www.apmiindia.org/storagebox/images/Important/Update-SEBI%20CSCRF%20Circular%20dated%2020th%20Aug'24.pdf

3. **Media release and Circular issued by BSE & NSE**:
   - https://www.apmiindia.org/storagebox/images/Important/Media%20Release%20and%20Circular%20issued%20by%20BSE%20and%20NSE.pdf

4. **CSCRF Presentation by APMI:**
   - https://www.apmiindia.org/storagebox/images/Important/Presentation%20-%20CSCRF.pdf

5. **BSE MSOC- Blusapphire PPT:**
   - https://www.apmiindia.org/storagebox/images/Important/MSOC-%20BSE-%20BLUESAPPHIRE-%20PPT.pdf

6. **NSE MSOC- AUJAS PPT:**
   - https://www.apmiindia.org/storagebox/images/Important/MSOC-%20NSE-%20AUJAS-%20PPT.pdf

7. **Contact Details of the MSOC Teams**
   - https://www.apmiindia.org/storagebox/images/Important/Contact%20details%20of%20M-SOC%20Teams_1.pdf

8. **Important Update by APMI- 28th Feb'25:**
   - https://www.apmiindia.org/storagebox/images/Important/APMI-Important-CSCRF.pdf

9. **Extension on CSCRF- SEBI- 28th March'25:**
   - https://www.apmiindia.org/storagebox/images/Important/Extension%20towards%20Adoption%20of%20CSCRF.pdf

10. **Clarification from SEBI- 30th April'25 :**
    - https://www.apmiindia.org/storagebox/images/Important/Clarifications%20on%20CSCRF%20for%20SEBI%20Regulated%20Entities%20-%2030th%20April'25_1.pdf

11. **Policy Templates & Control Document provided by APMI:**
    - www.apmiindia.org > Member Login > Menu > CSCRF Policy Templates

12. **FAQs on Policy templates provided by APMI:**
    - https://www.apmiindia.org/storagebox/images/Important/FAQs%20on%20CSCRF%20Policies%20templates%20provided%20by%20APMI.pdf

13. **FAQs on CSCRF issued by SEBI:**
    - https://www.apmiindia.org/storagebox/images/Important/FAQ's%20on%20CSCRF%20.pdf

14. **Analysis of FAQs on CSCRF & Cloud Framework:**
    - www.apmiindia.org > Member Login > Menu > Compliance Sutra > June 2025 > Brief Analysis of FAQs on CSCRF & Cloud Framework

Disclosures:

1. It is important to note that APMI’s role in this initiative is limited to providing information & updates aligned with SEBI's CSCRF framework to its members.
2. Any customization at the entity level falls outside APMI's purview.
3. APMI will not be responsible for implementing any policy or process, nor will it make decisions on behalf of the PMS's management.
4. The APMI Member is responsible for appointing management-level personnel to oversee the services provided, evaluate their adequacy, review any findings or recommendations, and monitor ongoing activities.
5. You are requested to kindly check with your consultant/internal team for the execution of the above-mentioned matter.

______________________________**End of the Document**______________________________