भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Frequently Asked Questions (FAQs) on Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI REs and Framework for Adoption of Cloud Services by SEBI REs

Preface

1. 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. The key objective of CSCRF is to address evolving cyber threats, to align with the industry standards, to encourage efficient audits, and to ensure compliance by SEBI REs.

2. In light of the queries and suggestions received and consultation held with REs, Frequently Asked Questions (FAQs) have been prepared on CSCRF and Framework for Adoption of Cloud Services by SEBI REs.

3. The objective of the FAQs is to provide better clarity on several concepts related to CSCRF. For ease of reference, these FAQs are categorised into subjects under following heads:
   - 3.1. Governance and CISO related guidelines
   - 3.2. Thresholds for REs' categorization
   - 3.3. Asset Inventory and Classification of Critical/ Non-critical systems
   - 3.4. VAPT and Patch Management
   - 3.5. Cyber Audit and Timelines
   - 3.6. Cyber Capability Index (CCI)
   - 3.7. Software Bill of Materials (SBOM)
   - 3.8. Outsourcing related guidelines
   - 3.9. Cloud Service Providers (CSPs) and Hosted Services
   - 3.10. COTS product testing
   - 3.11. Log Management, Data Security, and other Protect guidelines

3.12. ISO 27001 certification

3.13. Security Operations Centre (SOC) and Market-SOC (M-SOC)

3.14. Threat Intelligence

3.15. DC-DR Drills

3.16. Response and Recovery

3.17. Classification and Handling of Cybersecurity Incidents

4. These FAQs are in the nature of providing guidance on the Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs), and any explanation/ clarification provided herein should neither be regarded as an interpretation of CSCRF nor be treated as a binding opinion/ decision of the Securities and Exchange Board of India. Different facts or conditions may entail different interpretations. For full particulars of the CSCRF governing cybersecurity and cyber resilience, please refer to actual text of the Acts/ Regulations/ Circulars appearing under the legal framework section on the SEBI website.

June 11, 2025

Frequently Asked Questions (FAQs) on Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI REs and Framework for Adoption of Cloud Services by SEBI REs

These FAQs aim to address the most common queries/ questions SEBI REs have about the CSCRF and Framework for Adoption of Cloud Services by SEBI REs in a simple and understandable manner.

FAQs have been consolidated into following categories:

1. Governance and CISO related guidelines
2. Thresholds for REs' categorization
3. Asset Inventory and Classification of Critical/ Non-critical systems
4. VAPT and Patch Management
5. Cyber Audit and Timelines
6. Cyber Capability Index (CCI)
7. Software Bill of Materials (SBOM)
8. Outsourcing related guidelines
9. Cloud Service Providers (CSPs) and Hosted Services
10. COTS product testing
11. Log Management, Data Security, and other Protect guidelines
12. ISO 27001 certification
13. Security Operations Centre (SOC) and Market-SOC (M-SOC)
14. Threat Intelligence
15. DC-DR Drills
16. Response and Recovery
17. Classification and Handling of Cybersecurity Incidents

Governance and CISO related guidelines

1. **Are banks required to submit a certificate of compliance to SEBI? What specific aspects of the CSCRF or RBI cybersecurity framework need to be covered in the certificate?**
   Answer: Banker to an Issue (BTI) and SCSBs shall submit a certificate of compliance to SEBI on the cybersecurity guidelines issued by RBI. Banks which have taken other SEBI registrations, shall be required to comply with CSCRF (as applicable). However, as clarified in Q.29, the controls shall apply only to IT infrastructure, network, application, software, etc. being used for SEBI RE related activities.

2. **As per RBI's directions, Bank's CISO are reporting to their Executive Director (ED) in charge of Risk function. However, CSCRF mandates CISOs' of MIIs and Qualified REs to report directly to the MD/ CEO of their organisation. Can this specific exemption be given to such SEBI REs (operating also as Banks under RBI regulations) to make it uniform?**
   Answer: As per CSCRF guidelines, the level, grade, and standing of CISO shall be at least equivalent to CTO/ CIO for MIIs and Qualified REs. Accordingly, the reporting of CISO to ED or MD/ CEO as per organisational structure shall be deemed compliant.

3. **Can a group-level CISO be designated as the effective CISO for multiple entities within the same group, especially for small-size, QRE, and mid-size REs?**
   Answer: Yes, group level CISO can be designated as the effective CISO for multiple entities within the same group.

4. **CSCRF requires REs to mandatorily have a CISO. Is it acceptable for REs to hire a part-time CISO who simultaneously holds CISO position at multiple REs?**
   Answer: For the ease of compliance without any additional burden, REs are allowed to onboard a remote CISO, provided the personnel is only dedicated to one specific organisation and not managing more than one organisations simultaneously. Further, REs are restricted to onboard part-time CISO.

Thresholds for REs' categorization

5. **SEBI Circular *'Clarifications to Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs)' (SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2025/60)* dated April 30, 2025 has revised the criteria and thresholds for Depositories Participants (DPs) categorization? Table 2**

in aforementioned circular mentions a criteria as 'Other than Stock Brokers'. What all entities are covered under this criteria?

Answer: It is clarified that row 2 in Table 2 of the aforementioned SEBI circular where criteria is given as 'Other than Stock Brokers' covers following entities: Banks, NBFC, Mutual Funds, RTA, Financial Institutions, Custodians, Clearing Corporations, Public Financial Institution, State Finance Corporation.

Accordingly, the updated Table 2 of the aforementioned circular is as follows:

S. No	Regulated Entity	DP also registered as	Classification for CSCRF
1.	Depository Participant (DP)	Stock Broker	To be classified as per the criteria followed for stock brokers.
2.		Banks, NBFC, Mutual Funds, RTA, Financial Institution, Custodians, Clearing Corporations, Public Financial Institution, State Finance Corporation	Qualified RE

Where,

Financial Institution: As per 2(39) of Companies Act 2013, "financial institution" includes a scheduled bank, and any other financial institution defined or notified under the Reserve Bank of India Act, 1934 (2 of 1934)

State Financial Corporation: Corporation/Institution established under the provisions of section 3 of the State Financial Corporations Act, 1951 (63 of 1951)

Public Financial Institution: Institutions falling under the definition of public financial institutional as provided in section 2(72) of the Companies Act, 2013

6. **Does the criteria and thresholds for Stock Brokers issued vide SEBI circular *SEBI/HO/ITD-1/ ITD_CSC_EXT/P/CIR/2025/60 'Clarifications to Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs)'* dated April 30, 2025, cover both Client-based stock brokers and proprietary stock brokers?**

Answer: The criteria mentioned in Clause 2.1 in SEBI circular *SEBI/HO/ITD-1/ ITD_CSC_EXT/P/CIR/2025/60 'Clarifications to Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs)'* dated April 30, 2025, shall be applicable for client-based stock brokers in accordance with computation of trading volume as mentioned below:

   a. Each trading member's Aggregate turnover (Gross Level) during the Financial Year (April 1 to March 31) across Equity, Equity Derivative, Currency Derivatives and Commodity derivatives shall be considered.

b. For Equity Segment, Gross Traded Value = Buy Value + Sell Value (excluding Auction trades), shall be considered.
c. For all future contracts in Derivative Segments, Gross Traded Value = Buy Value + Sell Value, shall be considered.
d. For all option contracts in Derivative segments, Gross Traded Value =Buy Premium Value + Sell Premium Value, shall be considered.

6.1. For proprietary brokers (brokers who do not have any client), the following categorization shall be applicable:

S. No.	Parameters	Qualified REs	Mid-size REs	Small-size REs	Self-certification REs
1.	Amount of collateral/ assets with Clearing Corporations (CCs)	N.A.	More than Rs. 1000 Crores	More than Rs. 10 Crores and less than Rs. 1000 Crores	Rs. 10 Crores and below

6.2. Further, in case trading member/ RE is engaged in Clientele as well as Proprietary Trading, such brokers shall be considered as client-based stock brokers and accordingly, the categorization provided vide SEBI circular *SEBI/HO/ITD-1/ ITD_CSC_EXT/P/CIR/2025/60 'Clarifications to Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs)'* dated April 30, 2025, shall prevail.

7. **How will SEBI address cases where the entity's categorization changes mid-year?**
Answer: Please refer Section 2 of CSCRF 'Thresholds for REs' categorization'. 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.

8. **If a Bank is having DP license under SEBI regulations, will the controls apply only to DP-related activities or to the entire IT infrastructure of the bank?**
Answer: The controls shall apply only to IT infrastructure, network, application, software, etc. being used for SEBI RE related activities.

Asset Inventory and Classification of Critical/ Non-critical systems

9. **Can the IT asset inventory be maintained manually (e.g., using Excel) instead of implementing an ITSM tool for organizations with minimal IT setups?**
   Answer: While automated ITSM tools provide greater efficiency and accuracy, smaller REs having lean structure with minimal IT infrastructure may maintain manual inventories, provided periodic updates and compliance with SEBI CSCRF asset management requirements are being ensured.

10. **What are the parameters for classifying Critical/ Non-critical systems?**
    Answer: The definition of '*Critical Systems*' has been provided in the *definitions* section. The same definition should be used for classifying REs' IT assets as critical/ non-critical. However, systems/ tools such as survey forms, loan calculators, etc. are internet-facing but still non-critical for REs business operations. Therefore, classification of such systems/ tools may be left to REs based on the risk assessment of such applications. Further, please refer CSCRF '*Identify: Asset Management: standard 4*' with their corresponding guidelines which states that Board/ Partners/ Proprietor shall approve the list of critical systems. In case of any ambiguity, REs may take inputs from their respective 'IT Committee' (please refer CSCRF Section 3 'IT Committee for REs': Page 44).

11. **Is it mandatory for REs to maintain all IT assets (hardware, software, digital assets, APIs, etc.) under a single ITSM tool, or can they use multiple tools based on feasibility and accessibility?**
    Answer: CSCRF does not explicitly mandate the use of a single ITSM tool for managing IT inventory. REs have the flexibility to use multiple tools for asset management based on feasibility and accessibility, provided they maintain comprehensive, up-to-date and accurate inventory. Please refer CSCRF '*Identify: Asset Management: standard 1 and 2*' with their corresponding guidelines.

12. **How should REs classify systems that are connected to critical systems but do not directly impact core business operations (e.g., ancillary systems)?**
    Answer: The definition of '*Critical Systems*' has been provided in CSCRF '*Definitions'* section. The same definition should be used for classifying REs' IT assets as critical/ non-critical. Further, REs should consider and assess factors such as impact of system failure on operations, sensitivity of data processed, potential security risks (e.g. PII data breach) and their connectivity to critical systems before classifying systems as critical/ non-critical.

13. **What is the expected approach for maintaining an inventory of cryptographic assets and prioritizing critical assets for Post-Quantum Cryptography (PQC) migration?**

Answer: It is envisaged that quantum computing may be a reality in near future and it may be able to break the encryption schemes widely used today. Thus, quantum computing may evolve into one of the biggest cybersecurity threats and it may potentially expose financial systems to cyber-attacks. While it is still uncertain when quantum technology would be adopted on a large scale, its potential as a cyber-threat to the securities market ecosystem is already a matter of concern. Therefore, CSCRF emphasizes the importance of maintaining a comprehensive inventory of cryptographic assets. REs should identify and document all assets utilizing cryptographic mechanisms, including data in transit and at rest, communication channels, and authentication systems. The inventory shall describe what cryptography is used by which application for what purpose. The inventory shall include keys, certificates, algorithms, etc. Prioritization for PQC migration should be based on the risk assessment, criticality of the asset, sensitivity of the information it protects, and its exposure to potential threats.

VAPT and Patch Management

14. **What is periodicity of Vulnerability Assessment and Penetration Testing (VAPT) and Cyber audit for Qualified Stock Brokers (QSBs)?**
    Answer: SEBI vide circular *'Enhanced obligations and responsibilities on Qualified Stock Brokers (QSBs)'* (*SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/24*) dated February 06, 2023 has designated certain stock brokers as a Qualified Stock Brokers (QSBs) to meet enhanced obligations and responsibilities. Therefore, the periodicity of VAPT and cyber audit for QSBs shall be half-yearly irrespective of the category they fall in as per CSCRF.

15. **What is the expected timeline for addressing vulnerabilities related to third-party applications or dependencies that are outside the control of REs?**
    Answer: The timeline for closure of vulnerabilities identified (irrespective of third-party applications or in-house) during VAPT activity is within three (3) months of submission of VAPT report. For more details, please refer Table 19 in CSCRF. REs are encouraged to include 'VAPT finding closure' related timelines in their SLA with third-party service providers to remain complied with CSCRF. REs may also consider compensatory controls like virtual patching as mentioned under Guideline 6 of '*CSCRF: Protect: Maintenance: Standard 3*'. Further, REs may also consider virtual patching guidelines from CERT-In where OEM patches have longer period of implementation subject to the confirmation from their respective *'IT Committees'*.

16. **How should vulnerabilities that are identified but not overdue be reported, and what is the expected format for such reporting?**
    Answer: Please refer Section 4.3. '*VAPT'* under '*CSCRF Compliance, Audit Report Submission, and Timelines*' in CSCRF. It mentions VAPT related reporting,

periodicity, and timelines. Further, the reporting format shall be as per **CSCRF: Annexure-A**.

17. **What are the timelines for closure of finding identified during VAPT activity?**
Answer: Please refer Section 4.3. '*VAPT'* under '*CSCRF Compliance, Audit Report Submission, and Timelines*' in CSCRF. It mentions VAPT related reporting, periodicity, and timelines. However, it is being clarified that:
    a. Vulnerabilities identified due to non-implementation of patches and falling under 'high' severity would be validated for non-compliances against the patch management timelines (1 week; please refer standard PR.MA.S3 and the corresponding guidelines specified under PR.MA: Guidelines in Part II of CSCRF). Such vulnerabilities can be discovered proactively by REs through OEMs website or notification from OEMs as per arrangements made.
    b. Other vulnerabilities observations apart from implementation of patches shall be validated for non-closure against the VAPT observation closure timelines (3 months). However, even for the closure of such findings, graded approach (based on the criticality; please refer section 4.3. '*VAPT'* under '*CSCRF Compliance, Audit Report Submission, and Timelines*') shall be followed.

18. **What are the patch deployment timelines for applications deployed on cloud?**
Answer: Requirements for patch management are provided at standard PR.MA.S3 and the corresponding guidelines specified under PR.MA: Guidelines in Part II of CSCRF (Page 116-117).
The responsibilities of CSP and RE for closure of vulnerabilities and deployment of corresponding patches shall be clearly demarcated in the contractual agreement.

19. **Is it mandatory to test patches in a non-production environment before deploying them to production and DR sites?**
Answer: CSCRF emphasizes the importance of testing patches in non-production environment before deploying them to DC and DR. This practice ensures that patches do not introduce unforeseen issues or conflicts in production environments, thereby maintaining stability and integrity.

Cyber Audit and Timelines

20. **Whether the periodicities mentioned in the CSCRF are based on calendar year or financial year?**
Answer: All the periodicities mentioned in the CSCRF are based on financial year.

21. **What should be the mechanism of reporting the compliances to SEBI?**

Answer: The reporting of the compliances for the Framework for Adoption of Cloud Services shall be done to the authority as per the existing mechanism of reporting for Cybersecurity Audit**.**

The cyber audit periodicity for REs is specified in Table 21 of section 4 (CSCRF Compliance, Audit Report Submission, and Timelines) of the Cybersecurity and Cyber Resilience Framework [Circular No. SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113] dated August 20, 2024.

Further, the reporting authority for cyber audit report submission is specified in Table 23 of section 4 of CSCRF.

22. **What is applicable audit timelines for SEBI REs w.r.t. CSCRF compliance and cyber audit?**

Answer: Please refer Section 4.4. '*Cyber Audit'* under '*CSCRF Compliance, Audit Report Submission, and Timelines*' in CSCRF. To verify the compliances with CSCRF, REs shall conduct the cyber audit after the end of audit period. For example: REs who have been mandated to conduct cyber audit once in a year, such REs shall the start the cyber audit for the period April'2025-March'2026 after March'2026.

23. **Which SEBI circular(s) shall be followed for audit of the period (April'2024-March'2025) or (April'2024-September'2024 and October'2024-March'2025) as per the applicability?**

Answer: Please refer Clause 10 of '*Clarifications to Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs)*' vide SEBI circular SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/ 2025/60 dated April 30, 2025. Therefore, any cyber audit conducted for audit period from FY 2025-26 onwards shall be as per the circular *SEBI/HO/ITD-1/ITD_CSC_EXT/P/ CIR/2024/113* dated August 20, 2024, read along with the clarifications issued.

REs have flexibility to undertake cyber audit for the period (April'2024-March'2025) or (April'2024-September'2024 and October'2024-March'2025), as applicable, in accordance with CSCRF or previously issued SEBI cybersecurity-related circulars.

24. **How should entities with multiple licenses (e.g. bank/ broker/ mutual fund) prioritize their category of compliance? Should the largest business by revenue dictate the overall entity's classification?**

Answer: Please refer point 23 of CSCRF Section 2 '*Thresholds for REs' categorization*' which mentions that in case an RE is registered under more than one category of REs, then the provision of highest category under which such an RE falls shall be applicable to that RE.

25. **A services where licenses have been obtained but the service is not operational, does the bank still need to comply with the relevant provisions of the circular?**
    Answer: The provisions of the circulars are applicable to all those intermediaries who are registered with SEBI in the capacity of intermediary. Whether the services of the intermediaries are operational or not it is their business decisions, the provision may continue to apply.

26. **If a cloud provider's "India region" routes encryption key management requests through a foreign country, does this violate SEBI's data sovereignty expectations?**
    Answer: Yes, such routing may violate SEBI's data sovereignty expectations. The framework mandates that encryption keys and key management operations must be handled within the boundaries of India to ensure compliance with regulatory requirements. REs should assess and verify the key management architecture of their CSPs and adopt solutions like Bring Your Own Key (BYOK) to maintain full control over encryption keys. It may be noted that SEBI is doing an active consultation to finalise the guidelines related to Data Localisation requirements.

27. **If RE having business in other sectors/ domains also, does the audit coverage includes entire IT infrastructure/ software/ applications of the RE or only limited to the IT infrastructure/ software/ application under the purview of SEBI?**
    Answer: The audit coverage shall be limited to RE's IT infrastructure/ software/ applications under the purview of SEBI. However, this shall be applicable only if infrastructure/ software/ applications are properly segregated. If there are any ancillary/ connected systems used for accessing/ communicating with systems under SEBI purview, those systems should also be covered under audit against CSCRF.

28. **Are open-source security testing tools along with licensed tools permissible for auditors?**
    Answer: The tools used by auditors (irrespective of licensed or open-sourced) shall be permissible as long as it is allowed to use those tools for commercial purposes without violating their terms of usage.

29. **Are there any restrictions on hiring auditors who provided consulting services to the RE in past two years?**
    Answer: Yes, please refer CSCRF *Annexure-D 'Audit Guidelines: Auditor Selection Norms'.*

Cyber Capability Index (CCI)

30. **CSCRF mandates MIIs and Qualified REs to develop automated tool and suitable dashboards for submitting automated compliance. What is the significance for this requirement?**
Answer: CSCRF has mentioned that MIIs and Qualified REs shall build an automated tool and suitable dashboard (preferably integrated with log aggregator) for submitting compliance. Automated dashboard integrated with log aggregator provides REs the flexibility to streamline their reporting and compliances and free from manual interventions and errors. It is also one of the parameters marked for Cyber Capability Index (CCI).

31. **How does the Cyber Capability Index (CCI) assessment to be conducted by MIIs and Qualified REs?**
Answer: MIIs shall conduct third-party assessment of their cyber resilience using CCI on a half-yearly basis. Qualified REs shall do self-assessment of their cyber resilience using CCI on a yearly basis. Please refer Standard 4 of '*Governance: Oversight (GV.OV)',* corresponding guidelines, and Annexure-K.

32. **How do decimal values handled in CCI score or SOC efficacy? How should REs calculate score if an undefined value is obtained during calculation?**
Answer: Score can be taken in decimal value up to two decimal places. Further, if an undefined value is obtained during any calculation, then the maximum or minimum (depending on parameter and corresponding formula) marks of that particular category shall be used for further calculation.
For example:
    i. In parameter 14 of CCI (Table 27), the formula is (Number of individuals' screened/total number of individuals having access to organization's information and information systems) ×100. Here, suppose if both the parameters are zero (0), then zero marks shall be awarded for this parameter.
    ii. In parameter 2 of CCI (Table 27), the formula is (Number of vulnerabilities mitigated/ Number of vulnerabilities identified)×100. Here, suppose if both the parameters are zero (0), then maximum marks shall be awarded for this parameter.

    However, it may be noted that highest score (if achieved) for any category will be equivalent to weightage of that particular category.

33. **If an entity is partially complaint, for example RE achieves a score of 30% against the target value of 50% where 5 marks have been allotted for the parameter, then how will the score be calculated in such cases for Cyber Capability Index (CCI) (Annexure-K)?**
Answer: Partial scoring is allowed for the CCI assessment purpose. Taking the above-mentioned example, RE shall be awarded 3 marks in such case.

34. **How to make the submission of specific standards such as Cyber Capability Index (CCI)? For ex: the periodicity of Red Teaming exercise is half-yearly of MIIs and Qualified REs. However, for few of the Qualified REs, the periodicity of Cyber audit is annual.**
    Answer: All the periodicities and compliances are based on financial year. Further, it should be noted that the compliances of all standards and guidelines shall be submitted along with cyber audit report to the respective reporting authority.

Software Bill of Materials (SBOM)

35. **Which software are covered under SBOM requirement? Is SBOM mandatory for off-the-shelf software or only for custom-developed applications? Is the SBOM requirement limited to applications installed in REs' data centres, or does it also apply to SaaS applications used by the organization?**
    Answer: SBOM shall be obtained for all the software/ applications required for core and critical business operations. Please refer standard 5 under Governance: Cybersecurity Supply Chain Risk Management (GV.SC.S5) and its corresponding guidelines.

36. **Do REs need to obtain SBOMs for in-house developed applications, or is this requirement limited to third-party software?**
    Answer: All software/ applications required for core and critical business operations (irrespective of in-house or third-party) shall have a SBOM which documents all (but not limited to) components, dependencies, data relationships, etc.

37. **How should REs handle the procurement of SBOMs for legacy systems or proprietary software where vendors are unwilling to provide such details?**
    Answer: SBOM has become a key component for software security management. Therefore, REs should obtain SBOM for all software/ applications used in core and critical business operations of the RE. Please refer standard 5 under Governance: Cybersecurity Supply Chain Risk Management and its corresponding guidelines which states that in case the SBOM cannot be obtained for the legacy or proprietary systems, the Board/ Partners/ Proprietor of the organization shall approve the same with proper limitation, rationale, and risk management approach.

Outsourcing related guidelines

38. **Will SEBI hold RE accountable if a third-party vendor breaches contract and violates CSCRF guidelines?**
Answer: REs shall be solely accountable for all aspects related to third-party services including (but not limited to) confidentiality, integrity, availability, nonrepudiation, security of their data and logs, and ensuring compliance with laws, regulations, circulars, etc. issued by SEBI/ Government of India. Accordingly, REs shall be responsible and accountable for any violations of the same.

39. **SEBI outsourcing guidelines mentions: Core IT support infrastructure/ activities for running the core activities of exchanges. Some REs are reading this as a restriction on REs to engage with CSP, where the RE does not own the environment. SEBI Cloud adoption circular does not clarify this but instead suggests that the framework will be seen as an addition to existing circulars/ guidelines and advisories. Can REs host their critical applications on the cloud?**
Answer: Please refer clause 5(i) and 5(iii) of SEBI Cloud Adoption Framework which mandates REs to evaluate the need, implications (financial, regulatory, etc.), risks, benefits, etc. of adopting cloud computing. The RE shall also conduct its due diligence with respect to CSPs beforehand and on a periodic basis to ensure that legal, regulatory, business objectives, etc. of the RE are not hampered. The due diligence shall be risk-based depending on the criticality of the data/ services /operations planned to be on boarded on cloud. Further, the analysis (including but not limited to comparative analysis, SWOT analysis, etc.) shall also be conducted on the type of cloud model to be adopted. The analysis should include relevant factors like (including but not limited to) the risks associated with various models, need, suitability, capability of the organization, etc. The above mentioned evaluations / analyses should be conducted keeping in mind that although the IT services/ functionality can be outsourced (to a CSP), REs are ultimately accountable for all aspects related to the cloud services adopted by it including but not limited to availability of cloud applications, confidentiality, integrity and security of RE's data and logs, and ensuring RE's compliance with respect to the applicable laws, rules, regulations, circulars, etc. issued by SEBI/ Government of India/ respective state government. Accordingly, the RE shall be held accountable for any violation of the same. The Cloud risk management approach shall provide details regarding the various risks of cloud adoption such as technical, legal, business, regulatory etc., and the commensurate risk mitigation controls which should be proportionate to the criticality and sensitivity of the data/operations to be on-boarded on the cloud.
Therefore, a comprehensive risk management should be undertaken by the RE to continually identify, monitor, and mitigate the risks posed by cloud computing. Further, while outsourcing the activities, following SEBI circulars related to outsourcing (as applicable), but not limited to, shall be complied with:

Date of Issuance	Title of the SEBI Circular
Sep 13, 2017	Outsourcing of activities by Stock Exchanges and Clearing Corporations
Dec 09, 2015	Outsourcing by Depositories
Dec 15, 2011	Guidelines on Outsourcing of Activities by Intermediaries

40. **What are the expectations regarding the cybersecurity supply chain risk management strategy/process for REs?**
Answer: REs shall establish a robust cybersecurity supply chain risk management strategy that includes:
    i. Put in place appropriate third-party service providers risk assessment and controls proportionate to their criticality/ risk.
    ii. Service Level Agreements (SLAs) and contractual obligations
    iii. Third-party service providers shall be mandated to follow similar or higher standards of information security.

41. **Does obtaining source code of all critical applications mandatory for SEBI REs?**
Answer: Please refer CSCRF '*Protect: Data Security: standard 6*' with corresponding guidelines on Page 108-109 of CSCRF. However, it is being clarified that REs shall obtain the source code of only those critical applications which have been developed and intended for their sole use and purpose only. Where obtaining of the source code is not possible, REs shall put in place a source code escrow arrangement or other equivalent arrangements to adequately mitigate the risk of default by the third-party service provider. REs shall ensure that all product updates and patches/ fixes are included in the source code escrow arrangement.

Cloud Service Providers (CSPs) and Hosted Services

42. **What is the obligation for auditing the CSP's subcontractors/vendors?**
Answer: Cloud may engage non-material subcontractors to support in their operations periodically. Separately, service providers also utilize sub-contractors for day-to-day upkeep activities, such as for janitorial services. In view of this multi-layer environment in which CSPs operate, this requirement should be strictly limited to material subcontractors. For clarification, a material subcontractor is a subcontractor to whom a service provider has subcontracted a portion of their Services, where the subcontractor's role is such that its failure to perform would have a significant effect on service provider's ability to provide its services in

accordance with the Service Providers obligations under their agreement with the RE.

43. **How does the CSP provide Audit rights to the Regulated Entities?**
Answer: Please refer clause 4(ii) in SEBI Cloud Adoption Framework which mandates to have an explicit and unambiguous delineation/ demarcation of responsibilities with respect to all activities (including but not limited to technical, managerial, governance related, etc.) of the cloud services between the RE and CSP.
Further, refer clause 1(vi).2 of SEBI Cloud Adoption Framework which mandates REs to conduct regular audits/ VAPTof its cloud deployments.

Whenever required (by RE/ SEBI), the CSP shall provide visibility to RE as well as SEBI into CSP's infrastructure and processes, and its compliance to applicable policies and regulations issued by SEBI/ Government of India/ respective state government.

Please refer Principle 7: Contractual and Regulatory Obligations of SEBI Cloud Adoption Framework. The contractual/agreement terms between RE and CSP shall clearly specify the provisions for sharing audit reports including system audit report, cybersecurity audit report or any other audit report as deemed necessary by RE for compliance of SEBI CSCRF and Cloud Adoption Framework.

44. **Can REs leverage to have managed services offered by the CSP if there are other open-source alternatives that map to the same solution?**
Answer: SEBI does not intend to dictate or restrict technology choices of the RE through these guidelines. The REs needs to assess and manage risks, as identified in the guidelines. There is no mandate to adopt equivalent open source solution through this guideline.

45. **What steps should REs take if a cloud provider's MeitY empanelment lapses mid-contract, but critical workloads are already hosted in their infrastructure?**
Answer: The Cloud Adoption framework mandates that REs establish robust contractual agreements with CSPs that ensure ongoing compliance with regulatory requirements. In case of a MeitY empanelment lapse, the RE should assess risks and develop an action plan that may include the following (but not limited to) - migration to a compliant CSP, renegotiation for compliance measures, or invoking exit strategies specified in the agreement. Additionally, regular audits should monitor the CSP's adherence to security and certification requirements.

46. **What escalation mechanisms exist if a cloud provider refuses to share forensic evidence during SEBI investigations citing jurisdictional privacy laws?**

Answer: CSPs must provide data access during investigations. REs must establish clear escalation procedures in service agreements, ensuring CSP cooperation in providing forensic evidence. If privacy laws like GDPR conflict with Indian requirements, CSPs should have measures to prioritize compliance with SEBI regulations for Indian operations.

47. **How do REs verify that PaaS/ SaaS providers claiming compliance with STQC-certified infrastructure do not indirectly utilize non-empaneled subcontractors (e.g., global CDNs or edge networks)?**

Answer: REs must ensure that the CSP uses only MeitY-empaneled infrastructure for all applicable cloud services. The SEBI framework mandates that agreements with PaaS/SaaS providers include clauses ensuring back-to-back compliance by all subcontractors and service providers. REs should conduct audits to verify that no non-compliant services are used.

48. **How can REs ensure of STQC certification at the availability zone level when cloud providers only allow region selection, not specific data centers?**

Answer: The Cloud Adoption framework emphasizes that storage and processing of data, including logs, must be done within data centres of MeitY-empaneled CSPs that hold valid STQC certification or equivalent audit status. While cloud providers typically allow selection at the region level, the Regulated Entity (RE) must obtain assurance from the CSP that all data centres within the chosen region meet STQC certification requirements. Furthermore, REs should document compliance through contractual agreements.

49. **Can stock exchanges and clearing corporation run regulated workloads on the cloud?**

Answer: As per the Cloud Adoption Framework, REs can run their regulated workloads on the cloud on the basis of its business needs and technology risk assessment. However, compliance should be ensured with the Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs), 2023. It is to be noted that although RE may run regulated workloads on the cloud, RE is solely accountable for all aspects related to the cloud services adopted.

50. **How do REs verify that PaaS/SaaS providers claiming compliance with STQC-certified infrastructure do not indirectly utilize non-empanelled subcontractors (e.g., global CDNs or edge networks)?**

Answer: REs must ensure that the CSP uses only MeitY-empanelled infrastructure for all services. Please refer clause 2(ii).3 of SEBI Cloud Adoption Framework.

51. **What is the process of empanelment for those IT/SaaS/PaaS service providers who host the applications on their own data centres?**
Answer: For service providers who have their own data centres outside India, compliance shall be maintained by the concerned RE against the technical specifications for ***"Hosted Services"*** provided in the Cyber Security and Cyber Resilience Framework (CSCRF) *[Circular No. SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113]* dated August 20, 2024.

52. **Is it mandatory for REs to use ANSI/ TIA-942 rated-4 servers for all workloads? Is it acceptable to use Tier-3 servers for development or testing purposes?**
Answer: Please refer CSCRF 'Definitions' section. The requirement has been mandated for hosted services. For development or testing purposes, REs and their hosted service provider can use Tier-3 servers as long as it is being ensured that these environment do not contain production data, customer data, etc. However, due caution is emphasized since, in many incidents, it has been observed that the attack got originated in development environment and later spread and compromised the production environment.

COTS product testing

53. **For COTS or in-house developed software, can REs decide whether to conduct DAST or SAST based on their risk assessment, especially for internal-use applications with compensating controls?**
Answer: For COTS or In-house developed software, REs shall ensure that DAST or SAST tests/ audits are being done by CERT-In empanelled IS auditing organisation.
Definition of COTS[1]: A software and/or hardware product that is commercially ready-made and available for sale, lease, or license to the general public.

Log Management, Data Security, and other Protect guidelines

54. **What are different types of logs which should be collected, and how should REs ensure the integrity and confidentiality of these logs?**
Answer: Please refer first guideline of PR.AA.S8 (Page 98) mentioned in CSCRF which states that: REs are advised to ensure that all logs sources are being identified and their respective logs are being collected. An indicative list of types of log data to be collected by REs is as follows: system logs, application logs,

[1] Reference:
https://www.cnss.gov/CNSS/openDoc.cfm?a=AV1qZPhA4QFAfJhLI5UEag%3D%3D&b=79F3ADF8D651749481CD192C11F0F55DA585068EDDD5BCC88ADCEEC491E7F925B0FC8D9126629DA92E9A18D643950B08

network logs, database logs, security logs, performance logs, audit trail logs, and event logs.

Further, REs shall be responsible and take adequate security measures while sharing any such logs.

55. **When does an RE need to encrypt data in use?**

Answer: Please refer clause 6.2.9.i.3 in SEBI Cloud Adoption Framework. Further, refer CSCRF guideline 1(a) (Page 105) of Protect: Data Security (PR.DS) corresponding to Standard 1-3. MeitY Guidelines for the procurement of cloud services *[The guidelines are published at https://www.ambud.meity.gov.in/assets/web_assets/Includes/files/5.%20Guidelines_Procurement_Cloud%20Services_v2.2.pdf][Link]* require services offered under SaaS provide tools / capability for encryption of data-at-rest, data-in-motion and data-in-use.

56. **Can KRAs adopt alternative or manual solutions for cybersecurity requirements if automated tools like BAS and CART are not feasible due to cost and operational constraints?**

Answer: KRAs have been categorised as Qualified REs for the CSCRF Compliance. Since they are falling under Qualified REs which implies having significant scale of operations and importance in Indian securities market ecosystem, automated tools like BAS and CART are required to maintain cyber resiliency.

57. **What are the baseline security requirements for mobile application security to ensure compliance?**

Answer: Baseline security requirements for mobile application security are provided at Standard 16 of *'PR.AA: Identity Management, Authentication, and Access Control'* and its corresponding guidelines.

ISO 27001 certification

58. **Is it mandatory for third-party providers to have ISO 27001 certification in order to conduct business with SEBI REs?**

Answer: Please refer guideline of PR.IP.S16 (Page 115). The scope for ISO 27001 certification shall include (but not limited to) PDC site, DR site, NDR site, SOC, and Colocation facility. If any of the aforementioned is being outsourced to third-party service providers, then it must be ensured that those third-party service providers are also ISO 27001 certified for the services being outsourced to them.

Security Operations Centre (SOC) and Market-SOC (M-SOC)

59. **REs having global presence and infrastructure may fall under small-size and self-certification REs categories based on their business in Indian securities market. Is it mandatory for such REs to get onboarded to Market-SOC?**
Answer: Such REs can leverage their group SOC services. However, they will be required to submit the SOC efficacy report periodically as mandated in CSCRF.

60. **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 periodically as mandated in CSCRF.

61. **Who will facilitate the enrolment process for the Market SOC, will it be managed by BSE and NSE?**
Answer: CSCRF has mandated both BSE and NSE to setup Market-SOC for smaller REs. Please refer following circular/ guidelines issued by BSE and NSE on Market-SOC:
    a. NSE: https://nsearchives.nseindia.com/content/circulars/MSD66154.pdf
    b. BSE: https://www.bseindia.com/markets/marketinfo/DispMediaRels.aspx?page=7f35cda4-c3c7-431d-bd1b-4637518da317

    REs' enrolment process will be facilitated by BSE and NSE.

62. **Is it mandatory for REs to deploy all tools listed in Annexure-N, such as Database Activity Monitoring (DAM), and what are the expected capabilities of these tools?**
Answer: The tools listed are the SOC technologies deployed to the SOC for continuous monitoring of security events and timely detection of anomalous activities. The tools should meet the desired functionalities and REs are expected to evaluate these tools before onboarding.

63. **Can affiliate entities of an RE rely on a common audit report for shared services like SOC, IT infrastructure management, and data centres to meet compliance requirements?**

Answer: Affiliate entities sharing services such as SOC, IT infrastructure, data centres may utilize a common audit report to demonstrate compliance, provided that:

i. Reports are in the same format as provided under CSCRF.
ii. The shared services are uniformly implemented across all affiliated entities.
iii. The audit report comprehensively covers the cybersecurity controls and measures put in place for SEBI RE with proper evidences.
iv. There is clear documentation detailing the shared services and the respective responsibilities for each entity.
v. REs shall ensure that all the shared services are covered under such common audit report.

64. **How should global organizations with centralized SOCs handle India-specific requirements? Does SEBI allow the use of firm wide data for global organizations to meet SOC efficacy requirements?**
Answer: For global REs, SEBI allows them to submit their global SOC efficacy provided the global controls are applied uniformly.

65. **For SOC efficacy, do REs need to consider only given list of SOC Technologies or can they add other security tools / technologies used by the entity such as IDAM, FIM, and SSO?**
Answers: REs are encouraged to add more tools and technologies as per the requirements and resiliency of their IT infrastructure and business needs; the prescribed format has kept the flexibility and provision for adding more technologies.

66. **Is Capacity utilization mentioned in DE.CM.Standard 4 related to IT function?**
Answer: Capacity utilization given under DE.CM.Standard 4 is related to aspects covering the monitoring of anomalous utilisation, alerts, unusual network traffic etc.

Threat Intelligence

67. **Can REs rely solely on threat intelligence shared by NCIIPC and CERT-In for their quarterly threat hunting activities, or is additional intelligence required?**
Answer: While threat intelligence provided by NCIIPC and CERT-In is invaluable, REs are also encouraged to supplement it with industry sources and internal threat hunting mechanisms to strengthen cybersecurity posture. REs may integrate threat intelligence from industry-specific feeds, commercial providers, and industry peers to analyse threat intelligence relevant to their specific operational environment.

DC-DR Drills

68. **Are scenario-based cybersecurity drills mandated in CSCRF same as Red/Blue teaming, or do they serve a different purpose?**
Answer: Please refer CSCRF '*Governance: Risk Management: standard 3*' with their corresponding guidelines. While both Scenario-based Cybersecurity drills and Red/ blue teaming are integral to REs' security posture, they serve different purposes. Scenario-based cybersecurity drills assess REs' incident response and recovery capabilities in various scenarios. Red Teaming focuses on simulation of real threats and attacks to identify vulnerabilities in RE's IT environment; whereas Blue Team focuses on analysing such attacks and defend the RE's IT environment from Red Team.

69. **Is it mandatory for REs to cover all cybersecurity incident scenarios in a single drill, or can they be spread across multiple drills within one audit period?**
Answer: REs shall ensure that all the cybersecurity incident scenarios are covered in one audit period and all the relevant stakeholders are present in those drills and know their roles and responsibilities.

70. **Can REs conduct table-top exercises or walkthroughs instead of live drills for scenario-based cyber resilience testing?**
Answer: No, live drills are to test the readiness in the event of cyber incidents and involves real-world simulation and is akin to DR drill whereas table-top exercises are theoretical resilience drills and focusses more on discussions and walkthroughs.

71. **Can REs define their own RTO and RPO based on a business impact analysis, or are they required to adhere strictly to the RTO of 2 hours and RPO of 15 minutes as mandated by CSCRF?**
Answer: Please refer Guideline of Standard 2 in '*Recover: Incident Recovery Plan Execution*': 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 for the resumption of critical operations. The RPO shall be 15 minutes. REs shall establish their recovery plans in line with the RTO and RPO specified.

Response and Recovery

72. **CSCRF requires to retain spare hardware in an isolated environment. Is this mandatory and how REs should manage the overheads associated with maintaining and updating such hardware?**

Answer: Please refer guidelines corresponding to RC.RP.S1 on Page 127-128 of CSCRF. Maintenance of regularly updated 'golden images' of critical systems and retaining spare hardware has been mandated to MIIs and Qualified REs as their business is critical to Indian securities market ecosystem.

73. **How should REs validate the effectiveness of their response and recovery plans during business continuity drills?**
Answer: The CSCRF emphasizes the importance of conducting regular business continuity drills to validate the effectiveness of response and recovery plans. These drills should simulate various disaster scenarios to test the organization's preparedness. Post-drill evaluations are crucial to identify gaps, assess response times, and implement improvements to enhance the overall resilience of the organization.

74. **Can REs use cloud-based high-availability solutions as an alternative to maintaining physical spare hardware for critical services?**
Answer: Yes, REs can use cloud-based high availability solutions as an alternative to maintain physical spare hardware for critical services. However, all the required compliances (including SEBI CSCRF and Cloud Adoption Framework) shall be met.

Classification and Handling of Cybersecurity Incidents

75. **Can REs use in-house forensic auditors (at the group company level) or is it mandatory for them to be CERT-In empanelled?**
Answer: For all the forensic audits, REs shall select auditors after due diligence for carrying out the forensic audit related work(s). Indian government forensic labs may also be engaged depending upon the requirement. REs shall engage third-party auditors for forensic analysis/ audits.

76. **Is forensic auditing required for all cybersecurity incidents, or only for critical incidents involving financial loss or severe impact?**
Answer: CSCRF has mandated that for all incidents classified as High or Critical, the RE shall submit a forensic audit/ investigation reports (Please refer CSCRF *Annexure-O: Classification and Handling of Cybersecurity Incidents*). For incidents classified as low or medium, forensic report shall be submitted if the Root Cause Analysis (RCA) is inconclusive or if the SEBI/ HPSC-CS directs the same. (Please refer CSCRF *Annexure-O: Classification and Handling of Cybersecurity Incidents*). For all the forensic audits, REs shall select auditors after due diligence for carrying out the forensic audit related work(s). Indian government forensic labs may also be engaged depending upon the requirement.