4. CSCRF Compliance, Audit Report Submission, and Timelines:

This section provides details regarding submission of compliance with the CSCRF including ISO audit, VAPT, Cyber audit, etc. and the corresponding applicable timelines.

4.1. Compliance with the Standards/ Guidelines

Unless specified otherwise, the compliance reporting for CSCRF shall be done by the REs to their respective authority(ies) as per the existing mechanism, for example, MIIs shall submit the compliance with CSCRF to SEBI, stock brokers shall submit the compliance with CSCRF to stock exchanges, depository participants to shall submit the compliance with CSCRF to depositories, etc. Further, the compliance with the applicable standards and mandatory guidelines mentioned in CSCRF shall be as follows:

Table 15: Applicability and periodicity of standards mentioned in CSCRF

S. No.	Standard/ Guidelines and Clause	Applicability	Periodicity
1.	Cyber resilience third-party assessment using CCI (GV.OV.S4)	MIIs	Half-yearly
	Cyber resilience self-assessment using CCI (GV.OV.S4)	Qualified REs	Annually
2.	Submission of CCI self-assessment evidence by MIIs and Qualified REs (GV.OV.S4)	MIIs and Qualified REs	Within 15 days of completion of CCI assessment (based on the applicability defined above in point 1 and 2)
3.	REs Cybersecurity and cyber resilience policy review (GV.PO.S2)	All REs	Annually
4.	REs Cybersecurity risk management policy (GV.PO.S4)	All REs	Annually
5.	*IT Committee for REs* meeting periodicity (Guidelines for GV.PO – Guideline 9)	All REs except small-size, and self-certification REs	Quarterly
6.	REs' risk assessment (threat-based) (ID.RA.S2)	MIIs	Half-yearly
		Qualified, Mid-size REs	Annually
7.	User access rights, delegated access and	MIIs and Qualified REs	Quarterly

S. No.	Standard/ Guidelines and Clause	Applicability	Periodicity
	unused tokens review (PR.AA.S5)	Other REs	Half-yearly
8.	Review of privileged users' activities (PR.AA.S11)	MIIs and Qualified REs	Quarterly
		Other REs	Half-yearly
9.	Cybersecurity training program (PR.AT.S1)	All REs	Annually
10.	Review of RE's systems managed by third-party service providers (GV.SC.S4)	MIIs and Qualified REs	Half-yearly
		Other REs	Annually
11.	Functional Efficacy of SOC (DE.CM.S1 – Guideline 4)	MIIs and Qualified REs	Half-yearly
		Other REs who are utilizing third-party managed SOC or Market SOC services	Annually
12.	Red Teaming exercise (DE.DP.S4)	MIIs and Qualified REs	Half-yearly
13.	Threat hunting (DE.DP.S5)	MIIs and Qualified REs	Quarterly
14.	Cybersecurity scenario-based drill exercise for testing adequacy and effectiveness of recovery plan (RC.RP.S3)	MIIs and Qualified REs	Half-yearly
		Other REs	Annually
15.	Review of periodically and update their contingency plan, continuity of operations plan (COOP) (RS.MA.S3)	MIIs and Qualified REs	Half-yearly
		Mid-size and small-size REs	Annually
16.	Evaluation of cyber resilience posture (EV.ST.S5)	Mid-size and Small-size REs	Annually

Note: During cyber audit, auditors shall also validate the adherence to the above-mentioned periodicities.

4.2. ISO Audit and Certification

4.2.1. It is mandated (as per standard PR.IP.S16) that MIIs and Qualified REs shall obtain ISO 27001 (latest version) certification. Accordingly, all MIIs and Qualified REs shall obtain ISO 27001 within 1 year of issuance of CSCRF. The evidence of certification shall be submitted along with the cyber audit report to the authority(ies) as given below:

Table 16: Reporting authority for ISO certification evidence submission

S. No.	Regulated Entity	Reporting authority
1.	Stock Brokers / Depository Participants who are categorized as Qualified REs	Stock Exchanges / Depositories
2.	MIIs and rest of the Qualified REs	SEBI

4.3. VAPT[16]

The VAPT scope, periodicity and compliance has been defined in standard **DE.CM.S5** and the corresponding guidelines.

4.3.1. The VAPT reporting format has been attached at **Annexure-A**. It may be noted that along with the VAPT report, SEBI REs shall also submit the declaration from MD/ CEO (as given in **Annexure-A**). The reporting authority for VAPT report is as follows:

Table 17: Reporting authority for VAPT report submission

S. No.	Regulated Entity	Reporting authority
1.	Stock Brokers / Depository Participants	Stock Exchanges / Depositories
2.	IAs	BASL
3.	MIIs and rest of the REs	SEBI

4.3.2. REs shall plan their VAPT activity in 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 all such cases, the unaudited period shall be included in the current audit cycle. The periodicity of the VAPT activity for SEBI REs shall be as follows:

Table 18: VAPT periodicity of REs

S. No.	Regulated Entity	Periodicity
1.	REs which have been identified as '*Protected systems*' and/ or CII by NCIIPC	At least twice One VAPT activity shall be completed (including report submission, closure, and revalidation) in each half of the financial year (April to September and October to March)

[16] Unless otherwise specified, all audits mentioned in CSCRF have to be conducted by CERT-In empanelled IS auditing organization.

S. No.	Regulated Entity	Periodicity
2.	Rest of the REs	At least once VAPT activity shall commence in the first quarter of the financial year

4.3.3. The timeline for VAPT activity for SEBI REs shall be as follows:

Table 19: VAPT report submission and observations closure timeline

S. No.	Activity	Timeline
1.	Report submission of VAPT	VAPT report shall be submitted after approval from respective *IT Committee for REs*, within one (1) month of completion of VAPT activity.
2.	Closure of findings identified during VAPT activity	Within 3 months of submission of VAPT report A graded approach (based on the criticality of observations) shall be followed for closure of the observations found during VAPT.
3.	Revalidation of VAPT	Revalidation of VAPT shall be completed within 5 months of completion of VAPT.

4.3.4. The closure of vulnerabilities shall be regularly tracked by *IT Committee for REs*. Additionally, 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. REs are also expected to maintain risk register which shall be reviewed by the *IT Committee for REs*.

4.3.5. The report of revalidation of VAPT exercise, and open observations must be placed before the respective *IT Committee for REs* for their confirmation and appropriate directions.

Box Item 2: Categorisation of open observations w.r.t. VAPT and cyber audit

All open observations after follow-on audit of cyber audit and/ or VAPT shall be appropriately categorised (indicative categories are mentioned below). These open observations to be placed before the IT Committee for REs and shall be closed as per their timelines approved by the Boards/ Partners/ Proprietor.

Table 20: Indicative categories of open observations after follow-on audit

S. No.	Category	Example
1.	Absence of security control	MFA not implemented
2.	Security control exist but exceptions to the control	Data-at-rest and Data-in-motion encryption is present
3.	Security control in place but not consistently implemented	Asset inventory is being maintained but newly onboarded assets are not inventoried due to operational issues.

4.4. Cyber Audit

Cyber audit[17] here pertains to the audit conducted for verifying the compliance with CSCRF. MIIs and Qualified REs shall strive for building an automated tool and suitable dashboards (preferably integrated with log aggregator) for submitting compliance with CSCRF. The dashboard, once made, shall be available at the time of cyber audit, onsite inspection/ audit by SEBI or any agency appointed by SEBI.

Cyber audit shall cover 100% of the *critical systems* and 25% non-critical systems (chosen on a sample basis).

Box Item 3: Cyber Audit and Guidelines

To verify the REs' compliance with CSCRF, cyber audit has been mandated for applicable REs.
CSCRF includes the following:

1. *Standard format for cyber audit report*
2. *Standard format for exception reporting*
3. *Periodicity, cyber audit report submission, and observations closure timeline*
4. *Action taken on open observations in report*
5. *Auditor selection norms*
6. *IT Security Auditing Guidelines for REs*

In order to achieve uniformity in reporting across REs, the audit report format has been standardized and a standard exception reporting format has also been introduced.
It has been mandated to close all open cyber audit observations with 3 months of cyber audit report submission after approval from respective IT Committee for REs. The closure of audit observation shall be regularly tracked by IT Committee for REs. In cases of open observations, the auditor shall indicate if a follow-on audit is required to review the status of non-compliances.

4.4.1. 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. In all such cases, the unaudited period shall be included in the current audit cycle. The periodicity of conducting cyber audit for SEBI REs in a financial year shall be as follows:

[17] Unless otherwise specified, all certifications / audits mentioned in CSCRF have to be conducted by CERT-In empanelled IS auditing organization.

Table 21: Cyber audit periodicity for REs

S. No.	Regulated Entity	Periodicity
1.	MIIs, Qualified REs	At least twice in a year
2.	Mid-size REs and Small-size REs who are providing IBT or Algo trading facility	
3.	Rest of the REs	At least once in a year

4.4.2. The timeline of the cyber audit for SEBI REs shall be as follows:

Table 22: Cyber audit report submission and observations closure timeline

S. No.	Activity	Timeline
1.	Cyber audit report submission	The final cyber audit report shall be submitted after approval from respective *IT Committee for REs*, within 1 month of completion of cyber audit.
2.	Closure of findings identified during cyber audit	Within 3 months of cyber audit report submission A graded approach (based on the criticality of observation) shall be followed for closure of the observation found during cyber audit.
3.	Follow-on audit	The follow-on audit shall be completed within 5 months of completion of cyber audit.

4.4.3. Cyber audit report shall be submitted by all applicable REs. The auditor selection norms and format for CSCRF compliance submission has been attached at **Annexure-B**. Along with the cyber audit report, SEBI REs shall also submit the required declaration from MD/ CEO (as given in **Annexure-B**).

Table 23: Reporting authority for cyber audit report submission

S. No.	Regulated Entity	Reporting authority
1.	Stock Brokers / Depository Participants	Stock Exchanges / Depositories
2.	IAs	BASL
3.	MIIs and rest of the REs	SEBI

4.4.4. The closure of audit observations shall be regularly tracked by *IT Committee for REs*. Additionally, all open observation after 3 months of completion of cyber audit shall be approved by *IT Committee for REs* and shall be closed before start of next audit exercise.

4.4.5. The follow-on audit report and open observations must be placed before their respective *IT Committee for REs* for their confirmation and appropriate directions.

4.4.6. REs categorised as self-certification shall be required to conduct only VAPT audit through CERT-In empanelled IS auditing organisation and no other audit is required to be conducted. Self-certification (format attached at **Annexure-P)** shall be submitted for compliance with the applicable CSCRF provisions signed by RE's authorised signatory (MD/ CEO/ Board member/ Partners/ Proprietor).

4.5. Market SOC

4.5.1. The Market SOC shall be set up in accordance with the CSCRF requirements and shall ensure that participating REs are in compliance with CSCRF as applicable to them.

4.5.2. The Market SOC shall be setup:

a. Mandatorily by NSE and BSE
b. Optionally by NSDL and/ or CDSL

4.5.3. The report of functional efficacy of Market SOC shall be provided by BSE and NSE (also NSDL and CDSL, if applicable) to SEBI on a periodic basis.

4.5.4. The timeline for setting-up of Market SOC shall be January 01, 2025.