Annexure-B: Cyber Audit Report Format

Cyber audit report format for compliance submission

NAME OF THE ORGANISATION: <Name>

ENTITY TYPE: <Intermediary Type>

ENTITY CATEGORY: <Category of the RE as per CSCRF>

RATIONALE FOR THE CATEGORY: <>

PERIOD OF AUDIT: <>

NAME OF THE AUDITING ORGANISATION: <Name>

Date on Which Cyber Audit Report presented to 'IT Committee for REs' : <Date>

RE's Authorised signatory declaration:

I/ We hereby confirm that the information provided herein is verified by me/ us and I/ we shall take the responsibility and ownership of this cyber audit report.

Further, this is to certify that:

a. *Comprehensive measures and processes including suitable incentive/ disincentive structures, have been put in place for identification/ detection and closure of vulnerabilities in the organization's IT systems.*
b. *Adequate resources have been hired for staffing our Security Operations Centre (SOC).*
c. *There is compliance by us with CSCRF.*

Signature:

Name of the signatory:

Designation (choose whichever applicable): <MD/ CEO/ Board member/ Partners/ Proprietor>

Company stamp:

Annexures:

1. Minutes of the Meeting (MoM) of 'IT Committee for REs' <Date> in which the cyber audit report was approved.
2. Cyber audit report as submitted by the auditor

Table of Contents

This is to be submitted by the auditor on the company's letter head.

1. **Auditor's Declaration**

TO WHOM SO EVER IT MAY CONCERN

This is to declare and certify that I am a Partner/Proprietor of firm <Name of the Auditing Organization> with CERT-In empanelment from <Date> to <Date>. I have conducted Cyber audit for <Name of the RE> period <….> as per the requirements of SEBI.

Checklist for Cyber audit as required:

S. No.	Area	Details of the audit area	Is the Entity Compliant? (Yes/No)	Auditor's comments
1.	Cybersecurity and Cyber resilience policy			
2.	Asset Inventory			
3.	Risk assessment and Risk management			
4.	Supply chain risk management			
5.	Awareness and Training			
6.	Data security			
7.	Security continuous monitoring			
8.	SOC efficacy			
9.	Incident Management and Response			
10.	Incident recovery planning			

I confirm that the audit has been conducted as per the auditor's guidelines prescribed in CSCRF (Cyber Audit).

I also confirm that I have no conflict of interest in undertaking the above-mentioned audit.

For and on behalf of

Name:

Contact no.:

Place:

Date:

2. Executive Summary
   <Auditing Organization to provide an executive summary of the findings>

3. Scope of audit/Terms of reference (as agreed between the auditee and auditor), including the standard/specific scope for audit:-

   3.1. List of SEBI Circulars/ Guidelines/ Advisories/ Letters covered:

S. No.	SEBI circular/ letter/ advisory	Issue date

   3.2. List of all IT infrastructure and geographical locations (including IT systems of PDC, DR, Near site, Co-lo facility) covered under audit

S. No.	List of IT infrastructure/ Geographical locations/ Third-party vendors	Details (assets ID, asset name, applications, etc.) of the Infrastructure assessed
1.	PDC	
2.	DR	
3.	Near-site	
4.	Co-location Facility (if applicable)	
5.	Cloud Infrastructure	
6.	Third-party service provider	
7.	Others	

   3.3. Any other specific item(s)

4. Methodology/ Audit approach (audit subject identification, pre-audit planning, data gathering methodology, sampling methodology etc. followed by the Auditing Organization)

5. Summary of findings (including identification tests, tools used and results of tests performed)

S.No	Number of Non-conformity	Number of observations	Risk rating				Any other comments
			Critical	High	Medium	Low	
1							

6. Control-wise Compliance status of SEBI CSCRF:

S.No	Standards prescribed by SEBI CSCRF (Clause number and text)	Description of Finding(s)/ Observation(s)	Name of the system belongs to RE or third-party vendor	Status/nature of findings	Risk rating (C/H/M/L) of the findings	C/I/A affected	Test cases used	Root Cause Analysis	Impact analysis	Auditor recommendations/ Corrective actions	Deadline of corrective action(s)	Management response	Whether similar issue was reported in the last three audits.	*List of documentary evidence including physical inspection/ sample size taken by the auditor
1	GV.OC.S1													
2	GV.OC.S2													
…														
N	EV.ST.S5													

*Explicit reference to the key auditee organisational documents (by date or version) including policy and procedure documents

7. A brief description of the above-mentioned compliance requirements is as follows-
   i. Standards prescribed by SEBI CSCRF (or any other cybersecurity circular/ letter/ guidelines) (Clause number and text)- The clause corresponding to this observation w.r.t CSCRF (or any other cybersecurity circular/ letter/ guidelines) issued by SEBI.
   ii. Description of findings/observations – Description of the findings in sufficient details, referencing any accompanying evidence
   iii. Name of system belongs to RE or vendor-(Self Explanatory term)

iv. Status/ Nature of Findings – The category can be specified, for example:
   a. Non-compliant (Major/Minor)
   b. Work in progress
   c. Observation

v. Risk Rating of the finding - A rating shall be given by the auditing organization for each of the observations, based on its impact and severity, to reflect the risk exposure as well as the suggested priority for action

Rating	Description
CRITICAL	The failure shall have impact on the system delivery resulting in outage of services offered by the RE.
HIGH	Represents weakness in control with respect to threat(s) that is/are sufficiently capable and impacts asset (s) leading to regulatory non-compliance, significant financial, operational and reputational loss. These observations need to be addressed with utmost priority.
MEDIUM	Represents weakness in control with respect to threat(s) that is/are sufficiently capable and impacts asset (s) leading to exposure in terms of financial, operational and reputational loss. These observations need to be addressed within a reasonable timeframe.
LOW	Represents weaknesses in control, which in combination with other weakness can develop into an exposure. Suggested improvements for situations not immediately/directly affecting controls. .

vi. C/I/A Affected **–** The principles of Confidentiality/ integrity/ availability affected due to issued left unaddressed**.**

vii. Test cases used **–**The details of test cases used for arriving at this observation. The test cases may also be provided as annexures with the report, if required.

viii. Root Cause analysis – A detailed analysis on the cause of the non-conformity.

ix. Impact Analysis **–** An analysis of the likely impact on the operations/ activity of the RE.

x. Auditor recommendations/ Corrective actions **–** The actions to be taken (by the RE) to correct the non-conformity.

xi. Deadline of corrective action(s) **-**The RE shall specify the deadline not only for the corrective action(s) to be taken on the system(s) where NC/ observation was found, but also specify the deadline for corrective action on systems with related functionalities/ configurations where similar observations could have been found/are found.

xii. Management response – Management action plan/taken to address the observation and/ or implementation of auditor's recommendation

xiii. Whether similar issue was reported in the last three audits – Yes/ No

xiv. List of documentary evidence including physical inspection/ sample size taken by the auditor

8. Format for exception reporting by the RE: These exceptions shall be approved by the *IT Committee for REs*

S. No.	Standard of CSCRF	Description of non-compliance	Auditor observation	Auditor recommendation	Management comments	Comment of 'IT Committee for REs'	Comments of Board of RE	Comments of Board of Trustee (wherever applicable)	Status of non-compliance (open/closed)	Repeat observation in last 3 audits	Deadline for corrective action	Risk category of non-compliance

9. The audit report shall also include the following-

9.1. Audit report shall provide terms of reference (ToR) of audit which shall indicate the scope/perimeter of the coverage of the systems audited in the cyber audit report regarding the compliances checked including areas (but not limited to) computer hardware, business applications, software, cyber governance, linkage with vendor systems/ other REs' systems like stock brokers, RTAs, Fund Accountants, email systems, etc.

9.2. Audit report shall include open observations from previous audits and comments of auditors for compliances checked for the same.

9.3. The auditor shall mention in the audit report the methodology adopted to check compliance. Further, the reason for disagreement between auditor and management, if any, shall also be recorded in audit report.

10. Any other relevant comments by the auditor:

11. Conclusion of cyber audit