SEBI Cybersecurity Audit Readiness Checklist

iVALUE

SEBI's cybersecurity audit requirements mandate that MIIs and Qualified REs undergo bi-annual third-party assessments, while other REs must conduct at least one annual audit (SEBI Guidelines on Cybersecurity, Section 6). Our checklist provides a streamlined approach to meet these regulations, including certified auditor requirements, structured audit processes, and secure documentation practices. Adhering to these guidelines will enhance your cybersecurity readiness and ensure compliance.

AUDIT FREQUENCY

Ensure compliance with SEBI-mandated audit frequencies based on entity classification.

- **MIIs and Qualified REs:** Schedule third-party cyber resilience assessments every six months Implement Cyber Capability Index (CCI)
- **Mid-Size and Smaller REs:** Plan for at least two cybersecurity audits per year Ensure focus on internet-based trading entities
- **All Other REs:** Schedule at least one cybersecurity audit annually

AUDITOR SELECTION

Choose CERT-In empanelled auditors for cybersecurity assessments.

- Identify and engage CERT-In empanelled auditors
- Verify auditor's certification in cybersecurity assessments

AUDIT EXECUTION

Execution phase involves in-depth evaluation of cybersecurity measures.

- Prepare for assessment of IT systems, applications, and processes
- Ensure availability of necessary documentation and access

AUDIT PLANNING

Proper planning ensures comprehensive coverage and efficient use of resources.

- Define audit scope
- Identify systems to be audited
- Set audit objectives
- Select appropriate audit methodology and tools

AUDIT MANAGEMENT

Execution phase involves in-depth evaluation of cybersecurity measures.

- Establish structured audit management processes
- Implement systems for audit planning, execution, and follow-up

REPORTING AND FOLLOW-UP

Execution phase involves in-depth evaluation of cybersecurity measures.

- Prepare for timely submission of audit reports to SEBI (within one month of audit completion)
- Establish process for addressing identified issues within specified timelines
- Create system for tracking and implementing remediation measures

iVALUE

DOCUMENTATION AND EVIDENCE STORAGE

Maintain comprehensive records of audit findings and remediation efforts.

- Set up system for maintaining comprehensive audit documentation
- Ensure easy access to stored evidence for future audits or inspections

Implement secure storage for audit evidence, including:

- Logs
- Reports
- Supporting documentation

CONTINOUS IMPROVEMENT

Ongoing improvement is key to maintaining strong cybersecurity resilience.

- Establish process for reviewing audit findings
- Create system for tracking progress in improving cybersecurity resilience
- Implement mechanism for incorporating lessons learned into security practices

COMPLIANCE VERIFICATION

Be prepared for SEBI reviews and potential follow-up inspections.

- Prepare for potential SEBI review of audit reports
- Be ready to provide additional information if requested
- Plan for possible follow-up inspections by SEBI

SPECIFIC FOCUS AREAS

Every RE and MII must focus on their unique infrastrcuture

For MIIs and Qualified REs	For Mid-Size and Smaller REs	For all REs
Prepare to demonstrate high level of cybersecurity preparedness	Focus on robust security measures for internet-based trading	Be prepared to show efforts in staying ahead of emerging threats

AUDITOR'S DECLARATION IN CYBERSECURITY AUDIT REPORT

The SEBI CSCRF requires all REs to conduct cybersecurity audits and obtain an auditor's declaration

The auditor's declaration is a formal statement affirming the accuracy, integrity, and completeness of the audit findings in a cybersecurity audit report.

The auditor's declaration helps build trust in the audit process and assures stakeholders that the audit was conducted in accordance with applicable standards and guidelines