CDSL/IS/DP/POLCY/2025/681 **October 09, 2025**

IMPLEMENTATION OF SEBI CSCRF CIRCULAR FOR VAPT REPORT SUBMISSION

DPs are advised to refer to SEBI circular No: *SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113 August 20, 2024* & CDSL communique no. CDSL/OPS/DP/POLCY/2024/468 August 21, 2024 on 'Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs) and subsequent clarification circulars issued by SEBI dated December 31, 2024, March 28, 2025, April 30, 2025, August 28, 2025, and Frequently Asked Questions (FAQ) dated June 11, 2025.

As per point no 4.3.2 of the CSCRF circular dated August 20, 2024, RE / Depository Participants shall plan their VAPT activity in the beginning of the financial year. RE / Depository Participants shall ensure that no audit cycle shall be left unaudited (if any) due to the change in categorization. In all such cases, the unaudited period shall be included in the upcoming/next audit cycle.

For the implementation of CSCRF guidelines for VAPT audit, following timelines have been prescribed in consultation with SEBI, for the conduct & submission of VAPT Report for Depository Participants falling under **Self-certification RE's, Small-size RE's, Mid-size RE's and Qualified RE's (not categorized as QSB's)**:

i) Once in a Year - Financial Year (April 2025 – March 2026):

Yearly Submission for the period ending March 31, 2026	**Due Date**
Conduct of VAPT through Cert-in Auditor	June 30, 2026
VAPT report shall be submitted to Depository after approval from respective IT Committee	July 31, 2026
Submission of ATR/Revalidation report through Cert-in Auditor providing closure status after approval from respective IT Committee	November 30, 2026

Further, the timelines for the conduct & submission of VAPT report for Depository Participants categorised as QSB by any Stock Exchange or RE / Depository Participants which have been identified as 'Protected systems' and/or CII by NCIIPC are as follows: -

ii) Half-yearly period-April 2025 – September 2025 (applicable to QSBs & protected REs)

VAPT for Half Yearly period ending September 30, 2025	Due Date
Conduct of VAPT through Cert-in Auditor and report shall be submitted to Depository after approval from respective IT Committee	December 31, 2025
Submission of ATR/Revalidation report through Cert-in Auditor providing closure status after approval from respective IT Committee	March 31, 2026

iii) Half-yearly period- October 2025 – March 2026 (applicable to QSBs & protected REs)

VAPT for Half Yearly period ending March 31, 2026	Due Date
Conduct of VAPT through Cert-in Auditor and report shall be submitted after approval from respective IT Committee	June 30, 2026
Submission of ATR/Revalidation report through Cert-in Auditor providing closure status after approval from respective IT Committee	September 30, 2026

RE / Depository Participants should note that the modified timelines mentioned above for conduct of VAPT & Closure of vulnerabilities along with approval by IT Committee are as per Pt no- 4.3.4 (Page No- 49) of CSCRF, which states that "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".

The comprehensive scope of VAPT shall include all critical assets and infrastructure components including (not limited to) Networking systems, Security devices, Servers, Databases, Storage Systems, Applications, Cloud deployments, Systems accessible through WAN, LAN as well as with public IP's, websites, etc. The detailed scope of VAPT and testing methodologies for conduct of VAPT activity (Half Yearly/Yearly) shall be in accordance with Annexure – L of the SEBI CSCRF circular dated August 20, 2024, same is enclosed as **Annexure–1**.

The updated formats of VAPT Audit report/Summary, Declaration from REs and Auditor, Assessment Details in accordance with SEBI CSCRF has been enclosed as **Annexure–2**. Further as per SEBI Circular no- SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2025/119 dated August 28, 2025- on Technical Clarifications to CSCRF for SEBI Regulated Entities (REs), REs shall NOT submit details of explicit vulnerabilities (detailed report) unless and otherwise asked for the details by SEBI/Depositories.

However, RE / Depository Participants are required to maintain records of detailed VAPT report as per format provided in Point 7 of Annexure- A of SEBI circular no. SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024, and retain records of VAPT report along with POCs for a minimum period of three years. The detailed report shall be required to submit by REs as & when sought by SEBI/Depositories.

For the conduct of VAPT and appointment of auditor/auditing organization, RE / Depository Participants are required to refer auditor selection norms provided in **Annexure-3**, which are in accordance with norms specified in SEBI Cir no- SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024.

Further, guidelines for submission of reports on online portal details shall be communicated through a separate circular.

All Depository Participants are advised to take note of the above to bring the provisions of this circular to the notice of the auditors and put in place adequate systems and procedures to ensure strict adherence to the compliance requirements.

Queries regarding this communiqué may be addressed to CDSL by emails to: dpinfosec@cdslindia.com and connect through our IVR Number 022-62343333.

For and on behalf of
Central Depository Services (India) Limited

sd/-

Mrugen Vijay Munjpara
Assistant Vice President – Information Security

Annexure – 1 VAPT Scope

Comprehensive Scope for Vulnerability Assessment and Penetration Testing (VAPT)

1. The scope of the IT environment taken for VAPT should be made transparent to SEBI/Depository and should include all critical assets and infrastructure components including(not limited to) Networking systems, Security devices, Servers, Databases, Storage Systems, Applications, Cloud deployments, Systems accessible through WAN, LAN as well as with public IP's, websites, etc.

   The scope should include (not limited to):

S. No.	VAPT scope
1.	VA of Infrastructure (Server, Storage, Network, etc.) - Internal & External
2.	VA of Applications-Internal & External
3.	External Penetration Testing-Infrastructure & Application
4.	WIFI Testing
5.	API Security Testing
6.	Network Segmentation
7.	VA & PT of Mobile applications
8.	OS & DB Assessment
9.	VAPT of Cloud implementation and deployments
10.	Configuration audit of infrastructure (like i.e. operating systems, databases & middleware, endpoint devices, network devices, security devices, cloud and firewall rule review etc.)

2. **Testing methodology:** Testing methodology used for assessment to be documented with supporting relevant records and evidences. The VAPT should provide in-depth evaluation of the security posture of the system through simulations of actual attacks on its systemsand networks. The testing methodology should adapt from the following:
   a. SEBI CSCRF
   b. National Critical Information Infrastructure Protection Centre (NCIIPC)
   c. CERT-In Guidelines
   d. The National Institute of Standards and Technology ("NIST") Special Publication 800-115
   e. Latest ISO27001
   f. PCI-DSS standards
   g. Open Source Security Testing Methodology Manual ("OSSTMM")
   h. OWASP Testing Guide

Annexure - 2

VAPT Report Format on the RE's letter head

REPORTING FORMAT FOR MARKET ENTITIES TO SUBMIT THEIR COMPLIANCE AND FINDINGS OF VAPT

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 VAPT Report presented to 'IT Committee for REs': <Date>

RE's Authorized 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 VAPT report.

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 theVAPT report was approved.
2. VAPT report as submitted by the auditor

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

Table of Contents

This is to be submitted by the auditor on the auditor'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 VAPT for <Name of the RE> period <….> as per the requirements of SEBI.The scope of VAPT covers following circulars/ guidelines/ advisories issued by SEBI/Depository:

Checklist for VAPT compliance as required:

S. No.	Assessment Area	Details (assets, applications, etc.) of the Audit area	Is the Entity Compliant? (Yes/ No)	Auditor's comments
1	VA of Infrastructure (Server, Storage, Network, etc) -Internal & External			
2	VA of Applications-Internal & External			
3	External Penetration Testing			
4	Wi-Fi Testing			
5	API Security Testing			
6	VA and PT of mobile applications			
7	Network segmentation testing			
8	OS and DB Assessment			
9	VAPT of cloud implementation			
10	Configuration audit of infrastructure (like i.e. operating systems, databases & middleware, endpoint devices, network devices, security devices, cloud and firewall rule review etc.)			

I confirm that the VAPT has been conducted as per the auditor's guidelines prescribed in this framework.

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

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 VAPT

Sr. No.	Type of Assessment	List the details of the assessment
1.	Vulnerability Assessment of Infrastructure (Server, Storage, Network, etc..) – Internal and External	//List the count of IPs audited
2.	Vulnerability Assessment of Applications – Internal and External	//List the count of IPs audited
3.	External Penetration Testing –Infrastructure and Applications	//List the count of IPs audited
4.	Wi-Fi Testing	//List the number of Wi-Fi access points/ routers/ devicesaudited
5.	API Security Testing	//List the APIs audited
6.	Network Segmentation Testing	//List the network segmentationaudited //List of the Network architecture diagram & its review
7.	VA and PT of Mobile Applications	//List the number of APK filesand IPA files audited
8.	OS and DB Assessment	// List the type and number ofOS and DBs audited.
9.	VAPT of Cloud implementation and Deployments	//Name the cloud service provider and list the IPs audited
10.	Configuration audit of infrastructure (like i.e. operating systems, databases & middleware, endpoint devices, network devices, security devices, cloud and firewall rule review etc.)	//List the systems for which configuration audit has beenconducted

4. Tools used:

4.1. *Name of the Tool*:
4.2. *Type*: Open source/ Commercial
4.3. *Operations*: manual/ automated/ both

5. Exclusions, if any:

Please enclose attachments regarding exclusions as approved by 'IT Committee for REs' along with MoM of the meeting where the exclusions were approved.

6. Summary of the VAPT Report:

6.1 Details of Vulnerability Assessment findings:

Sr. No.	Vulnerability Assessment Findings Details												
1.	Auditor (Name) for VA:												
2.	VA Start Date:												
3.	VA End Date:												
4.	Scope	Vulnerability Assessment											Auditor Remarks
5.		Number of Identified vulnerabilities					Closure Timelines	Open vulnerabilities (Shall be applicableduring final submission)					
6.		Critical	High	Medium	Low	Total		Critical	High	Medium	Low	Total	
7.	Critical Assets												
8.	VA of infrastructure (Server, Storage, Network, etc..) - Internal and External												
9.	VA of Applications - Internaland External												
10.	Wi-Fi Testing												
11	API Security Testing												
12.	Network Segmentation												
13.	VA of mobile applications												
14.	OS and DB Assessment												
15.	VA of cloud deployments												
16	Configuration Audit of infrastructure (like i.e. operating systems, databases & middleware, endpoint devices, network devices, security devices, cloud and firewall rule review etc.)												
17.	Others, please specify												

6.2 Details of Penetration Testing findings:

Sr. No.	Penetration Testing Findings Details												
1.	Auditor (Name) for PT:												
2.	PT Start Date:												
3.	PT End Date:												
4.	Scope	Penetration Testing											Auditor Remarks
5.		Identified vulnerabilities					Closure Timelines	Open vulnerabilities (Shall be applicableduring final submission)					
6.		Critical	High	Medium	Low	Total		Critical	High	Medium	Low	Total	
7.	Critical Assets												
8.	External Penetration Testing - Infrastructure and Application												
9.	PT of mobile applications												
10.	PT of cloud deployments												
11.	Others, please specify												

6.3 Risk Rating description

Rating	Description
CRITICAL	The failure has an 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.

Annexure - 3

Auditors Selection Norms for VAPT

a. Auditing Organisation/Entity must mandatorily be CERT-In empanelled'.
b. Auditor of Auditing Organisation/Entity must preferably have a minimum 3 years of experience in IT audit of Banking and Financial services preferably in the Securities Market. E.g. Stock exchanges, clearing houses, depositories, stockbrokers, depository participants, mutual funds, etc. The audit experience should have covered all the major areas mentioned under various cybersecurity frameworks and guidelines issued by SEBI from time to time. Auditing experience of the Cybersecurity Framework under ISO 27001 for an organization will be an added advantage.
c. The Auditor of Auditing Organisation/Entity must have experience in/ direct access to experienced resources in the areas covered under CSCRF. It is recommended that resources employed shall have relevant industry recognized certifications e.g. CISA (Certified information Systems Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, GSNA (GIAC Systems and Network Auditor), CISSP (Certified Information Systems Security professional) from International Information systems Security Certification Consortium, commonly known as (ISC)2.
d. The Auditor of Auditing Organisation/Entity shall have ISMS/ IT audit/ governance frameworks and processes conforming to leading industry practices like COBIT.
e. The Auditor & Auditing Organisation/Entity must not have any conflict of interest in conducting fair, objective and independent audit of the REs. It shall not have been engaged over the last two years in any consulting engagement with any departments/ units of the RE being audited.
f. The Auditor & Auditing Organisation/Entity may not have any cases pending against its previous auditees, which fall under SEBI's Jurisdiction, which point to its incompetence and/or unsuitability to perform the audit task.
g. The auditor of Auditing Organisation/Entity must have experience of performing VAPT.
h. The auditor of Auditing Organisation/Entity must compulsorily use only licensed tools.
i. The Auditing Organisation/Entity must compulsorily enter into a Non-disclosure Agreement (NDA) with the auditee. Under no circumstances, the data sought during the review or the audit report subsequently should leave the jurisdiction of India.

****