Circular No.: NSDL/POLICY/2025/0121 September 15, 2025

Subject: Implementation of SEBI CSCRF circular w.r.t. VAPT Audit Report Submission.

Attention of Participants is invited to SEBI Circular no. SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024, (ref : Circular No.: NSDL/POLICY/2024/0118 dated August 27, 2024) regarding 'Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs)'.

As per guidelines for submission of VAPT Audit Reports as part of the cybersecurity compliance requirements mandated under the CSCRF in the aforesaid circular, Participants are advised to adhere to the following guidelines concerning VAPT Audit Report submission to ensure compliance with SEBI's cybersecurity framework.

(i) Timeline/Periodicity: -

As per point no 4.3.2. of the aforementioned SEBI circular - 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. Based on the same and as per discussion with all Exchanges/Depositories the new periodicity is as below: -

Table - 1

Yearly Submission – DP who is a Non - Qualified Stock Brokers (QSBs) members	**Existing Due Date**	**New Due Date**
Conduct of VAPT through Cert-in Auditor.	30th November	30thJune
VAPT report shall be submitted to Exchange/Depositories after approval from respective IT Committee.	31st December	31st July
Submission of ATR (revalidation report) through Cert-in Auditor providing closure status after approval from respective IT Committee.	31st March	30th November

Table - 2

VAPT for First Half Yearly ending March 31 Submission - DP who is a Qualified Stock Brokers (QSBs) members	**Existing Due Date**	**New Due Date**
Conduct of VAPT through Cert-in Auditor and report shall be submitted to Depository after approval from respective IT Committee.	30th June	30th June
Submission of ATR (revalidation report) through Cert-in Auditor providing closure status after approval from respective IT Committee.	30th September	30th September

Table - 3

VAPT for Second Half Yearly ending September 30 Submission - DP who is a Qualified Stock Brokers (QSBs) members	**Existing Due Date**	**New Due Date**
Conduct of VAPT through Cert-in Auditor and report shall be submitted to Depository after approval from respective IT Committee.	31st December	31st December
Submission of ATR (revalidation report) through Cert-in Auditor providing closure status after approval from respective IT Committee.	31st March	31st March

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, Applications, 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 in accordance with SEBI CSCRF has been enclosed as **Annexure – 2.** Further, guidelines for submission of reports on online portals and other related details shall be communicated through a separate circular.

All members 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.

The above submission of VAPT shall be applicable for Financial Year ending with March 31, 2026 & onwards, hence Non-QSB (Non - Qualified Stock Brokers) members shall conduct VAPT for Financial Year -25-26 during April -June 2026 and submit the report as per timelines mentioned in Table-1. There shall be NO Change for conduct of VAPT & closure timelines for QSB (Qualified Stock Brokers) members.

For and on behalf of
National Securities Depository Limited

AROCKIARAJ Digitally signed by AROCKIARAJ
Date: 2025.09.15 12:47:57 +05'30'

Arockiaraj
Manager

Enclosure: Two

FORTHCOMING COMPLIANCE			
Particulars	**Deadline**	**Manner of sending**	**Reference**
Investor Grievance Report (Monthly)	By 10th of the following month	Through e-PASS	Para 22 of 'Grievance Redressal' chapter and Para 27 of 'Internal Controls/Reporting to NSDL/SEBI' chapter of NSDL Master Circular for Participants
Compliance report w.r.t Same Mobile number and/ or email address captured for multiple accounts. (Monthly)	Before 27th of following month	Through Email.	Para 23 of 'Miscellaneous' chapter of NSDL Master Circular for Participants.
Action Taken Report (ATR) (If applicable) – For Annual System Audit & Annual Cyber Audit (Annually)	September 30th	Through e-PASS	Circular No.: NSDL/POLICY/2025/0077 dated June 17, 2025 and Circular No.: NSDL/POLICY/2025/0078 dated June 17, 2025

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, Applications, 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-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 (operating systems, databases & middleware, endpoint devices, network devices, security devices, cloud and firewall rule review)

2. **Testing methodology:** The VAPT should provide in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and 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

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

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-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 (operating systems, databases & middleware, endpoint devices, network devices, security devices, cloud and firewall rule review)			

I confirm that the VAPT has been conducted as per the auditor's guidelines prescribedin 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 – 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 (operating systems, databases & middleware, endpoint devices, network devices, security devices, cloud and firewall rule review)	//List the systems for which configuration audit has been conducted

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 Committeefor REs' along with MoM of the meeting where the exclusions were approved.

6. Summary of the VAPT Report:

6.3. 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											
5.		Number of Identified vulnerabilities					Closure Timelines	Open vulnerabilities (Shall be applicable during final submission)					Auditor Remarks
6.		Critical	High	Medium	Low	Total		Critical	High	Medium	Low	Total	
7.	Critical Assets												
8.	VA of infrastructure - 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 (operating												

	systems, databases & middleware, endpoint devices, network devices, security devices, cloud and firewall rule review)												
17.	Others, please specify												

6.4. 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 applicable during 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												

`

7. Detailed Report

Detailed report to be submitted for all the items in the scope as per the below-mentioned format:

Sr. No	**URL/ Application name**	**Type of Risk (Critical/ High/ Medium/ Low)**	**Type of Assessment (As reported in point no 6 i.e. Summary)**	**Observations/Vulnerability**	**Reference (CVE/ CWE/ OWASP/ Best practise)**	**EPSS /SSVC score**	**Impact**	**Recommendations**	**Status of Vulnerability (Open/Close)**	**Management comments with specific closure timelines**
1										
2										

8**. 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.