NATIONAL COMMODITY & DERIVATIVES EXCHANGE LIMITED

Circular to all members of the Exchange

Circular No. : NCDEX/Member Tech Compliance-010/2026

Date : May 15, 2026

Subject : Submission of VAPT Report for the FY 2025-26

To All Trading Members,

This is with reference to SEBI Circular No-SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024, on 'Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs) and subsequent clarification circulars dated December 31, 2024, March 28, 2025, April 30, 2025, August 28, 2025, and Frequently Asked Questions (FAQ) dated June 11, 2025 issued by SEBI and Exchange circular NCDEX/Member Tech Compliance-018/2025dated September 26, 2025, on 'Submission of VAPT Report for the FY 2025-26'.

As per point no 4.3.2 of the CSCRF circular dated August 20, 2024, REs/trading members shall plan their VAPT activity at the beginning of each financial year. RE's/trading members 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 current audit cycle.

For the implementation of CSCRF guidelines for VAPT audit by REs, following timelines have been prescribed in consultation with SEBI, for the conduct & submission of VAPT Report for trading members 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 01, 2025 to March 31, 2026):

Yearly Submission	**Due Date**
Conduct of VAPT through Cert-in Auditor	June 30, 2026
Report shall be submitted after approval from respective IT Committee	July 31, 2026
Submission of ATR/Revalidation report through same Cert-in Auditor providing closure status after approval from respective IT Committee (If Applicable)	November 30, 2026

Note: VAPT activity shall be initiated by the REs after Financial Year (April 2025 – March 2026)

Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

Further, there shall be no change in the timelines for the conduct & submission of VAPT report for trading members categorised as **QSBs and REs which have been identified as 'Protected systems' and/or CII by NCIIPC.** The submission timelines are as follows: -

ii) Half-yearly period- October 01, 2025 – March 31, 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 same Cert-in Auditor providing closure status after approval from respective IT Committee (If Applicable)	September 30, 2026

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/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/trading members shall NOT submit details of explicit vulnerabilities (detailed report) unless and otherwise asked for the details by SEBI/Exchanges.

However, Trading Members/REs 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/trading members as & when sought by SEBI/Exchanges.

For the conduct of VAPT and appointment of auditor/auditing organization, RE's/Trading Members 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, trading members and appointed auditor are requested to take note of SEBI Circular No- HO/13/19/12(1)2026-ITD-1_CIMGI/10873/2026 dated May 05, 2026, on "Advisory on Emerging Advanced Artificial Intelligence (AI) Tools for Vulnerability Detection".

Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

Trading members are requested to take note of Annexure A of Exchange Circular No. NCDEX/MEMBER INSPECTION-009/2026 dated April 17, 2026, regarding actions for non-compliances observed in periodic submissions made by Trading Members/REs related to submission of VAPT Report. The details of financial disincentive(s)/ penalties/ disciplinary action(s) have been provided in **Annexure-4.**

Additionally, with reference to Exchange Circular no-NCDEX/COMPLIANCE-051/2025 dated September 29, 2025, regarding technology-based sharing mechanisms for common submissions among exchanges, Members of the Exchange who are also registered with NSE shall submit their Cyber Security & Cyber Resilience Audit report to NSE only. Members of the Exchange who are not registered with NSE shall continue to make submissions to the Exchange as per existing process on email ID-infosec@ncdex.com.

All members are advised to take note of the above & 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.

For and on behalf of
National Commodity & Derivatives Exchange Limited

Ravindra Shetty
Senior Vice President – Member Tech Compliance

For further information / clarifications, please contact

1. Customer Service Group on toll free number: 1800 26 62339
2. Customer Service Group by e-mail to : askus@ncdex.com

Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

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/Exchanges 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, critical endpoints, 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, critical 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") SpecialPublication 800-115
e. Latest ISO27001
f. PCI-DSS standards
g. Open Source Security Testing Methodology Manual ("OSSTMM")
h. OWASP Testing Guide

Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road,
Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

Annexure – 2

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

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.

Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

Table of Contents

Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road,
Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

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/Exchanges:

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, critical endpoints, 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, critical 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 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 (Server, Storage, Network, critical endpoints, etc.) – Internal and External	//List the count of IPs audited

Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

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, critical endpoint devices, network devices, security devices, cloud and firewall rule review etc.)	//List the systems for which configuration audit has beenconducted

4.Tools used:

1.1. *Name of the Tool*:

1.2. *Type*: Open source/ Commercial

1.3. *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.

Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

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 applicable during final submission)					
6.		Critical	High	Medium	Low	Total		Critical	High	Medium	Low	Total	
7.	Critical Assets												
8.	VA of infrastructure (Server, Storage, Network, critical endpoints, 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												

Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road,
Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

16	Configuration Audit of infrastructure (like i.e. operating systems, databases & middleware, critical endpoint devices, network devices, security devices, cloud and firewall rule review etc.)												
17.	Others, please specify												

Note:

1. Trading Member shall ensure that the vulnerability assessment i.e. VA of critical endpoint devices (Laptop/desktop) is covered under point 8 & configuration audit i.e. CA of critical endpoint devices (Laptop/desktop) is covered under point 16.
2. Trading Member shall provide the total count of identified vulnerabilities in all the mentioned assessments (Point no. 8 to 17, wherever applicable) under 'Critical Assets' row i.e. point no. 7.
3. Trading Member shall mention the count of identified vulnerabilities in VA and PT of the Mobile, Cloud, External Application and External Infrastructure in their respective 'Vulnerability Assessment Findings Details' table 6.1 & 'Penetration Testing Findings Details' table 6.2.

Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road,
Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

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 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												

Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road,
Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

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.

Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

Annexure 3

Auditors Selection Norms for VAPT

a. Auditing Organization/Entity must mandatorily be CERT-In empaneled'.

b. Auditor of Auditing Organization/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. A Cert-In empaneled auditing organization can audit the REs for a maximum period of three consecutive years. Subsequently, the said auditing organization shall be eligible for auditing the REs again only after a cooling period of two years.

d. The Auditor of Auditing Organization/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.

e. The Auditor of Auditing Organization/Entity shall have ISMS/ IT audit/ governance frameworks and processes conforming to leading industry practices.

f. The Auditor & Auditing Organization/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.

g. The Auditor & Auditing Organization/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.

h. The auditor of Auditing Organization/Entity must have experience of performing VAPT.

i. The auditor of Auditing Organization/Entity must compulsorily use only licensed tools.

j. The Auditing Organization/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.

Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

Annexure 4

Actions for non-compliance observed in periodic submissions made by Trading Members/ REs related to submission of VAPT Report

Non-submission of VAPT report and/or compliance report:

Details of Contravention	Action in case of first instance first instance	Action in case of repeat instance
Delay/Non-submission of VAPT report and/or Compliance report (ATR) within the due date.	1.Charges Rs. 1,500/- per day for Non QRE & Rs. 3,000/- per day for QRE from the due date till first 7 calendar days or submission of report, whichever is earlier. 2.Charges of Rs. 2,500/- per day for Non QRE & Rs. 5,000/- per day for QRE from 8th calendar day after the due date to 21st calendar day or submission of report, whichever is earlier. 3.In case of non-submission of report till 21st calendar days, new client registration shall be prohibited and notice of 7 calendar days for disablement of trading facility till submission of report, shall be issued. 4.The disablement notice issued to the member will be shared with all the Exchanges for information. 5.In case of non-submission of report by 28th calendar day, Member shall be disabled in all segments till submission of report.	2nd Time & Onwards -Levy of applicable monetary penalty along with an escalation of 50%. In case of non-submission of report till 21st calendar days, new client registration shall be prohibited and notice of 7 calendar days for disablement of trading facility till submission of report, shall be issued. The disablement notice issued to the member will be shared with all the Exchanges for information. In case of non-submission of report by 28th calendar day, Member shall be disabled in all segments till submission of report.

Non-closure of VAPT report and/or compliance report:

Details of Contravention	Action in case of first instance first instance	Action in case of repeat instance
Non- closure of each Critical/High/Medium/Low vulnerabilities, as reported in Compliance Report/ ATR of VAPT by closure due date	a) For Self Certification Regulated Entity - Low Risk - Rs. 1,000/- Medium Risk - Rs. 3,000/- Critical/High Risk - Rs. 5,000/ b) For Small- Sized Regulated Entity - Low Risk - Rs. 2,000/-	

Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

	Medium Risk - Rs. 6,000/- Critical/High Risk - Rs. 10,000/ c) For Mid- sized Regulated Entity - Low Risk - Rs. 5,000/- Medium Risk - Rs. 15,000/- Critical/High Risk- Rs. 25,000/ d) For Qualified Regulated Entity (QREs) - Low Risk - Rs. 10,000/- Medium Risk - Rs. 30,000/- Critical/High Risk - Rs. 50,000/ (For Low Risk - If certification is provided on efficacy of compensatory controls no penalty, else penalty per vulnerability as mentioned above shall be applicable. Subject to closure of the same before start of period of next VAPT.) Apart from the monetary penalty mentioned above, if High/ Critical/Medium vulnerability is not closed by member within 21 days from the due date of submission of compliance report, new client registration shall be prohibited and notice of 7 days for disablement of trading facility shall be issued. If the vulnerability is not closed during this notice period, then member shall be disabled in all segments till closure of the vulnerability. The disablement notice issued to the member will be shared with all the Exchanges for information.	

Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com