Part III: Structured Formats for CSCRF Compliance

Annexure-A: 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 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 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 the VAPT report was approved.
2. VAPT report as submitted by the auditor

Table of Contents

Annexure-A

This is to be submitted by the auditor on the RE'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:

Checklist for VAPT compliance as required:

S. No.	Area	Details (assets, applications, etc.) of the Audit area	Is the Entity Compliant? (Yes/ No)	Auditor's comments
1.	Vulnerability Assessment			
2	External Penetration Testing			
3.	Wi-Fi Testing			
4.	API Security Testing			
5.	VA and PT of mobile applications			
6.	Network segmentation testing			
7.	OS and DB Assessment			
8.	VAPT of cloud implementation			
9.	Configuration audit			

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**

S. 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/ devices audited
5.	API Security Testing	//List the APIs audited
6.	Network Segmentation Testing	//List the network segmentation audited
7.	VA and PT of Mobile Applications	//List the number of APK files and IPA files audited
8.	OS and DB Assessment	// List the type and number of OS and DBs audited.
9.	VAPT of Cloud implementation and Deployments	//Name the cloud service provider and list the IPs audited
10.	Configuration audit	//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 Committee for 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:

S. 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 - Internal and External												
9.	VA of Applications - Internal and External												
10.	WiFi 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												
17.	Others, please specify												

6.4. Details of Penetration Testing findings:

S. 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 (to be submitted only when sought by SEBI):

S. No	URL/ Application Name	Type of Risk (Critical/ High/ Medium/ Low)	Observations/ Vulnerability	Reference (CVE/ CWE/ OWASP/ Best Practice)	EPSS/ SSVC score	Impact	Recommendations	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.