



Head Office – Near Gandhi Sagar, Mahal, Nagpur, 440018.

NOTICE INVITING QUOTATION

Shikshak Sahakari Bank Ltd., Nagpur invite Quotations from vendors for “Vulnerability Assessment and Penetration Testing (VAPT) Services” for Bank’s IT infrastructure/applications, interested vendors are requested to send their sealed quotations with all terms & conditions to the address mentioned below.

Sr. No.	Particulars	Branches
1.	Vulnerability Assessment and Penetration Testing (VAPT) Services for Bank’s IT infrastructure/applications, including identification of security vulnerabilities, penetration testing, risk assessment and submission of detailed VAPT report. Re-testing / Verification of identified vulnerabilities after remediation and submission of final compliance/re-testing report.	Itwari, Kamal, Medical, Sitabuldi, Dharampeth, Kampthi, Khamla, Nandanvan, Sadar, Bhagwaghar, Mhalginagar, Hingna, Hingna – Ext, Ramtek, Katol, Saoner, Chandrapur, Ballarpur, Warora, Umred, and Head Office (Total – 21 Sites)

Note: Annexure – 1 containing the detailed Scope of Work for Vulnerability Assessment and Penetration Testing (VAPT) is enclosed below. Vendors are required to carefully review the scope mentioned in Annexure and ensure that their proposal covers all the specified requirements.

Envelop to be quoted with: “Vulnerability Assessment and Penetration Testing (VAPT) Services”

Last Date for submission: 28/09/2026 before 04:00 p.m.

Address to send sealed quotations:

The Chief Executive Officer
Shikshak Sahakari Bank Ltd., Head Office,
Gandhi Sagar, Mahal, Nagpur - 440018

By order
Chief Executive Officer
Shikshak Sahakari Bank Ltd.

Annexure – 1

PART 1 – Summary of audit activities

Serial no.	Audit details	Quantity/ Number of Units
1.	Web Applications	4
2.	Thick Client - Desktop Application	0
3.	APIs	2
4.	Mobile Apps (Android / IOS)	2
5.	Source Code Audit	3
6.	Network Penetration Testing	29
7.	Servers/Virtual Machines	18
8.	Switches	27
9.	Routers	2
10.	Workstations/PCs/Laptops/LAN	360
11.	CCTV/ Biometric Devices	28
12.	IDS/IPS/Firewall	29
13.	Storage Devices (SAN) – (NAS)	1
14.	OT Systems	-
15.	Configuration Audit Servers/Virtual Machines	-
16.	Database Audit	2
17.	Configuration Audit Network Devices etc.	29
18.	Load/Stress Testing	-
19.	Cyber Security Framework Audit	1
20.	DC / DR Audit	1
21.	Network Architecture Review	1
22.	Red Team	-
23.	UIDAI Audit	-
24.	SAR Audit/Data Localization Audit	-
25.	Functionality Audit	-
26.	Forensic Audit	-
27.	Branch Audits	-
28.	Application Control Audit	-
29.	Firewall Rule base Audit	29
30.	AUA / KUA Audit	-
31.	ATM Malware Audit	-
32.	Data Migration Audit	1
33.	Policy Review	1
34.	Online Scanning, Anti-phishing, anti-rogue, dark web services	1
35.	Swift Audit	-
36.	ISO 27001/20000-1/22301 Consultancy & Certification	Yes
37.	SOC Type1 /Type 2 Consultancy & Certification	-
38.	Cyber Security Training	1
39.	Specific one-time audit – Regulatory or Client needed	1
40.	Any other type of assignment not mentioned above -like Tab, Electronic Product, Certifying Authority, Web Trust etc.	1
41.	Tape Library	-

Additional Information (If below mentioned audit needs to be conducted)

Penetration Testing:

Sl.NO	ITEM	DESCRIPTION
1.	Name of the Application	Swift 6.3
2.	Authorization No. of roles & types of privileges for the different roles.	Lot
3.	No. of Static and Dynamic Pages in each URL	STATIC PAGES: 2 DYNAMIC PAGES: Multiple
4.	No. of forms in the application (Module wise)	Lot
5.	No. of Input fields	Lot

API Testing:

Sl.NO	ITEM	DESCRIPTION
1.	Which Method is Used (GET, POST)	Yes (Both)

Mobile Application Penetration Testing:

Sl.NO	ITEM	DESCRIPTION
1.	No. of roles & types of privileges for the different roles.	Multiple
2.	Provision for e-commerce and/or payment gateway	-
3.	Site users (closed user group and/or open to public)	Open to public
4.	No. of Screens in app	Lot
5.	No. of forms in the application (Module wise)	Lot

Source Code Review:

Sl. No.	PREREQUISITE	PARTICULAR
1.	Name of the application(s)	Swift 6.3
2.	Size of the application(s)	-
3.	Lines of code (approx.)	-
4.	platform used to develop the application(s)	-

Please Note: Audit need to be performed 2 times for VA (Vulnerability Assessment) and 1 time for PT (Penetration Testing) both VA and PT need to be performed Onsite.