

Jalore Nagrik Sahakari Bank Ltd.

Head office : Rajendra Nagar Road, Near Jalore Club, Jalore 343001

Telephone : 02973-223407, Helpline No. 9079806434

Website: www.jalore.bank.in

Email: headoffice@jalore.bank.in

Sr/JNSB/ 2311

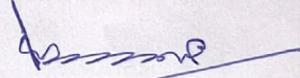
DATE ..12/3/2026

Tender Notice

Jalore Nagrik Sahakari Bank Ltd. invites sealed proposals from CERT- In empanelled information security Auditing Organization for conducting an IT & Cyber security GAP assessment, IS and VAPT Audit of the Bank in accordance with Reserve Bank of India (RBI) guidelines and CERT-In Advisories. Last Date of Submission of bid is 23.03.2026. The Bank will prefer the applications from the experienced entity in the requisite audit system. For detailed please visit bank website.

S.No.	Description	Minimum Professional Qualification	Minimum work Experience
1	IS Audit	CISA	5 Year
2	VA-PT Audit	CISSP	
3	GAP Assessment	ISO 27001 Lead Auditor CERT-IN empanelled CEH or Equivalent	

* Experience in conducting Audits for Urban Co-Operative Banks will be Preferred.



(Parmanand Bhatt)
Chief Executive officer



TENDER NOTICE

SUBJECT: VAPT/IS/GAP ASSESSMENT AUDIT 2026-2027

Scope of Work

The selected CERT-In empanelled Information Security Auditing Organization shall conduct IT & Cyber Security GAP Assessment, Information Systems (IS) Audit, and Vulnerability Assessment & Penetration Testing (VAPT) of the Bank's IT infrastructure in accordance with the guidelines issued by the Reserve Bank of India, applicable regulatory requirements, and relevant CERT-In advisories.

The audit shall include review, evaluation, and testing of the Bank's information systems, cyber security controls, and regulatory compliance framework, including but not limited to the following areas:

1. GAP Assessment

The GAP Assessment shall cover the Bank's compliance with RBI cyber security framework and related regulatory requirements. The assessment shall include:

- Review of IT Governance structure and Information Security Framework.
- Evaluation of Cyber Security controls in line with RBI Cyber Security Framework for Urban Cooperative Banks.
- Assessment of policies, procedures, and internal controls related to IT and Information Security.
- Review of risk management processes and cyber security risk assessment practices.
- Evaluation of vendor and third-party risk management controls.
- Compliance verification with applicable RBI circulars, advisories, and CERT-In guidelines.

2. Information Systems (IS) Audit

The IS Audit shall include a detailed review and validation of the Bank's IT systems and controls, including:

- Review of IT infrastructure architecture and network design.
- Assessment of Core Banking System (CBS) security and access controls.
- Review of user access management, authentication mechanisms, and privilege management.
- Evaluation of data protection mechanisms, backup procedures, and disaster recovery arrangements.
- Review of log management, monitoring mechanisms, and incident response processes.
- Assessment of IT asset management and system configuration controls.

3. Vulnerability Assessment & Penetration Testing (VAPT)

- The VAPT shall be conducted on critical IT assets of the Bank including but not limited to:



- Network infrastructure including routers, switches, firewalls, and related interfaces.
- Core Banking System infrastructure and supporting servers.
- Internet Banking, Mobile Banking, and web applications (if applicable).
- Bank website and externally accessible applications.
- Internal network and critical systems.
- Security testing of endpoints such as PCs and terminals.
- The testing shall be conducted using recognized industry standards such as OWASP methodology and other accepted security testing frameworks.

4. Payment Systems Security Review

Security review of the Bank's payment systems and related infrastructure, including:

- RTGS and NEFT interface security controls.
- Integration points with payment gateways or switching infrastructure.
- Authentication and encryption mechanisms used in payment transactions.
- Review of security controls implemented for digital banking transactions.

5. Network and Security Infrastructure Review

The audit shall include assessment of the Bank's security infrastructure such as:

- Firewall configuration and rule review.
- Network segmentation and perimeter security controls.
- Endpoint protection mechanisms.
- Security device configuration and policy review.

6. IT Policies and Procedures Review

Review and evaluation of the Bank's IT and Information Security policies including:

- Information Security Policy
- Access Control Policy
- Incident Response Policy
- Backup and Disaster Recovery Policy
- Vendor Management Policy
- Cyber Security Policy

7. Privacy and Data Protection

Assessment of mechanisms implemented for protection of sensitive information, including:

- Data protection and confidentiality controls.
- Secure data storage and transmission mechanisms.
- Procedures for secure disposal of documents and digital media containing sensitive information.

8. Deliverables

The selected auditor shall submit the following:

- Detailed GAP Assessment Audit Report.
- Vulnerability Assessment and Penetration Testing Report.
- Identification of control gaps and associated risk ratings (High / Medium / Low).
- Recommendations and remediation plan for identified issues.
- Executive summary for management and Board review.



Additional Eligibility & Compliance Conditions

1. CERT-In Empanelment

The bidder must be an Indian Computer Emergency Response Team (CERT-In) empanelled Information Security Auditing Organization and must submit a valid empanelment certificate along with the proposal.

2. Relevant Experience

The bidder should have minimum 5 years of experience in conducting Information Systems Audit, GAP Assessment, and VAPT for Banks / Financial Institutions / Urban Cooperative Banks.

Preference will be given to organizations having prior experience in conducting RBI-compliant cyber security audits for Urban Cooperative Banks.

3. Application /Bid will be opened by the Bank Management as per decision of concerned Committee at Head Office of the Bank.

4. All taxes will be applicable as per the norms.

5. The Bank does not bind itself to accept the tender and reserves to itself the right to reject any or all the tenders received within assigning of the reasons thereof.

6. Payment Terms & Out of Expense: Clearly Mentioned in Proposal.

