BSNL : 2204543, 2202976/ (M) 94601-46227
Email ID- headoffice@recbjaipur.com, website : www.recbjaipur.com
GSTIN- 08AAAAT0446Q2Z3
दी रेलवे एम्पलाईज को–ऑपरेटिव बैंक लि., जयपुर
The Railway Employee's Co-operative Bank Ltd. Jaipur
Head Office : Power House Road, Jaipur-302 006
(Registered Under Rajasthan Co-operative Societies Act.1953)
Established 1945 H.O. Jaipur.

IS Audit & VAPT Audit

The scope of work shall include not only the conduct of the audit, but also end-to-end support for remediation and compliance, as detailed below:

1. Audit Execution
The selected VAPT / IS Auditor shall conduct a comprehensive security audit covering applications, systems, network infrastructure, firewalls, antivirus/end-point security solutions, and other relevant IT assets, in accordance with applicable regulatory and industry standards.

2. Findings and Recommendations
The Auditor shall submit a detailed audit report highlighting all identified vulnerabilities, gaps, and non-compliances, along with risk classification and recommended corrective actions.

3. Compliance and Policy Support
- For all audit findings, the responsibility of the Auditor shall extend beyond reporting and shall include:
- Preparation, drafting, or updation of information security and compliance policies, as required
- Assistance in aligning policies with applicable regulatory and compliance requirements
- Guidance and support for effective policy implementation

4. Remediation and Implementation Support
- Except for procurement of hardware, software, or licenses (which shall be handled separately by CETIN), the VAPT / IS Auditor or their empanelled sister / group firm shall be responsible for:
- Implementation of corrective and preventive controls for audit findings
- Configuration, hardening, and remediation activities in systems, servers, networks, firewalls, and antivirus / endpoint security solutions
- Ensuring that identified vulnerabilities are addressed and closed in line with recommended best practices

5. Accountability
The Auditor shall be accountable for providing necessary technical and compliance support until closure of audit observations and shall assist in validation and re-testing, wherever applicable.

IS/VAPT Audit with Audit and 100% compliance including find policy making and implementation except procurement if requried, by certin auditor.

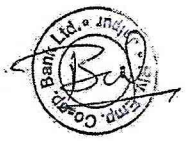
1- L 1 Switch	**--- 06 Nos.**
2- Shopos XGS 107 Firewall	**--- 05 Nos.**
3- Desktop PC	**--- 50 Nos. Approx**
4- Wireless Modem/Access Points	**--- 06 Nos.**
5- Antivirus Consol	**--- 01 Nos.**
6- Static IP	**--- 05 Nos.**
7- Website	**--- 01 Nos.**

Branch Location: Jaipur, Ajmer, Kota, Bandikui, Phulera and HO Jaipur.

The Railway Employee's Co-Operative Bank Ltd.,Jaipur

This scope comprehensively covers all IT assets deployed in the Bank including network devices, endpoint systems, and security equipment. The audit will ensure compliance with RBI guidelines and strengthen the Bank's cyber security posture.

Sr No.	Component	Scope	Audit Activities
01	Firewall	Security configuration & rule base review	Rule base analysis, port-based traffic control, logging & monitoring, patch updates
02	Switches (L1 & Dist.)	Network segmentation & configuration security	VLAN review, firmware updates, access control checks
03	Access Points (Wi-Fi)	Wireless security & authentication	Encryption standards, rogue AP detection, access log review
04	Static IP Configs	Exposure risk & secure allocation	NAT policy review, IP assignment validation
05	Client Machines/Nodes	Endpoint security	OS hardening, patch management, USB/Wi-Fi disablement, endpoint protection
06	Antivirus Console	Centralized malware protection	Policy enforcement, update frequency, monitoring of alerts
07	IDS/IPS / UTM	Intrusion detection & prevention	Signature updates, fine-tuning, intrusion attempt analysis
08	DMZ Architecture	Segregation of internal vs external traffic	Secure routing, firewall rules, monitoring
09	Logging & Monitoring	Audit trail & tamper-proof configuration	Log retention review, alert generation, access restrictions
10	VAPT Activities	Comprehensive vulnerability & penetration testing	Network scanning, port scanning, spoofing, DoS/DDoS, password testing, MITM attacks
11	Regulatory Compliance	Adherence to RBI, CERT-In, NCIIPC, NPCI guidelines	Mapping audit findings to regulatory advisories, ensuring compliance



Detailed Scope of IS Audit & VAPT (Bank Systems)

1. Network & Infrastructure Components

- **Firewall**: Rule base review, configuration security, port-based traffic control, logging & monitoring.
- **Switches (L1 & Distribution)**: Configuration review, VLAN security, access control, firmware updates.
- **Access Points (Wi-Fi)**: Authentication mechanism, encryption standards, rogue AP detection, access logs.
- **Static IP Configurations**: Review of allocation, NAT policies, and exposure risks.

2. Endpoint & Device Security

- **Client Machines / Nodes**: OS hardening, patch management, USB/Wi-Fi disablement, endpoint protection.
- **Antivirus Console**: Policy enforcement, update frequency, centralized monitoring.
- **Servers (if any hosted locally)**: OS security configuration, patch compliance, access control.

3. Security Devices & Controls

- **UTM / IDS / IPS**: Signature updates, fine-tuning, intrusion detection/prevention effectiveness.
- **DMZ Architecture**: Segregation of internal vs external traffic, secure routing.
- **Logging & Monitoring**: Review of log retention, alert generation, tamper-proof configuration.

4. Vulnerability Assessment & Penetration Testing (VAPT)

- **Network Scanning & Port Scanning.**
- **System Identification & Vulnerability Scanning.**
- **Access Control Mapping.**
- **DoS / DDoS Simulation.**
- **Password Strength & Authentication Testing.**
- **Application Security Testing**
- **Man-in-the-Middle & Browser Attack Simulation.**
- **Website / Web Application Testing** (as per OWASP standards).

5. Regulatory Compliance Review

- Ensure adherence to guidelines issued by **CERT-In, NCIIPC, RBI-CSITE, NPCI.**
- Verify compliance with RBI circulars on IT security, cyber resilience, and DEAF disclosures.