THE ASSAM CO-OPERATIVE APEX BANK LTD

Head Office : Panbazar, Guwahati - 781001 (Assam)

Phones: M.D- 2546413, EPABX- 2545092 , 2515013 , 2603591

E. Mail: md@apexbankassam.com

Website : www.apexbankassam.com

Inspection & Audit Department.E.Mail ID- (ia @ apexbankassam.com)

No. ACAB/HO/I&A/110/2025/ *Date :- 09/12/2025*

EXPRESSION OF INTEREST (E.O.I.)

Expression of Interest (E.O.I.) are invited from CERT-In empanelled Audit Firm for conducting Information System (I.S.) Audit in 67 branches of the Bank and H.O.

The broad scope of the audit is annexed herewith as Annexure-I.

Interested qualified Audit Firm may submit E.O.I. in the office of the undersigned on or before 24/12/2025.

The Assam Co-op. Apex Bank Ltd. Insp & Audit H.O. Guwahati

Sd/-

MANAGING DIRECTOR.

########

Scope of Audit Work:

The audit shall be conducted in compliance with CERT-In Cyber Security Audit Guidelines, NABARD IS Audit Framework circular no. 33/Dos -01/2015 (Annexure A & B), RBI/NABARD Cyber Security Framework, and applicable MeitY standardsalong with all relevant directives, circulars, and guidelines prescribed by NABARD and RBI.

The following categories of security audits and assessments, including but not limited to those listed below, are required and shall be deemed to fall within the scope of this document

1. **Comprehensive IT/IS & Cyber Security Audit** of the Bank's Data Centre (DC) at Guwahati, Disaster Recovery (DR) Site at STT Global, Kolkata, Head Office, and 67 Branches.
2. **Data Localization Audit for Payment Systems** as per RBI guidelines to ensure that all regulated payment data is stored, processed, and maintained within India.
3. **Cyber Awareness Training & Phishing Simulation Drill** for Bank employees to enhance cyber hygiene, identify social engineering threats, and measure employee readiness.

1.1 IT Infrastructure Audit (DC, DR, HO and Branches)

- Review of all policies, architecture diagrams, and documentation.

- Server/OS hardening, patch review, virtualization security.

- Network architecture review including firewalls, routers, switches, VLANs, segmentation, routing.

- SAN/NAS, backup systems, restoration testing.

- DR replication parameters, RPO/RTO validation, DR readiness.

- Branch infrastructure review including routers, endpoints, CBS access.

- Third-party integrations (IMPS, AEPS, CTS, PFMS, NACH, ATM Switch).

1.2 Application Security Audit

- Application coverage: CBS, ATM Switch, IMPS, AEPS, NEFT/RTGS, AML, PFMS, NACH, CTS, Positive pay, APIs.

- VAPT (internal & external), API security, input validation.

- Android Mobile Application VAPT (Positive Pay, FI Application)SAST& DAST, API

- Database audit: encryption, audit trails, privileged accounts.

- Source code review (FI application viz micro-ATM & AEPS)

- Full vulnerability discovery beyond OWASP Top 10/SANS 25.

1.3 Network Security Audit

- Review of firewall rule-base, NAT, IDS/IPS, WAF.

- Router/switch ACLs, SNMP security, routing integrity.

- VPN, IPsec/SSL tunnels, MFA for remote access.

- Internal & external VAPT covering all network devices and public endpoints.

- SIEM log ingestion completeness.

1.4 Cyber Security Controls Review

- SOC operations, incident response, threat intelligence.

- Log retention compliance (CERT-In 180 days minimum).

- Patch/change management review.

- Email security, DLP, USB restrictions.

- PAM review and privileged user monitoring.

- Endpoint security review.

1.5 Compliance Review

- NABARD Annexure A & B control mapping.

- RBI/NABARD Cyber Security Framework compliance.

- MeitYcompliance for logging and data protection.

1.6 Physical & Environmental Security

- Access controls, CCTV, environmental sensors (smoke, temperature, humidity).

- Fire safety, UPS, DG, HVAC.

- Physical security checks across DC, DR, HO, Branches.

1.7 Branch-Level IT/IS Audit (67 Branches)

- CCTV, Fire safety at Branches

- ATM security.

The Assam Co-op. Apex Bank Ltd. Insp & Audit H.O. Guwahati

- Endpoint hardening, patch status, antivirus/EDR.

- CBS access, maker-checker compliance.

2. RBI Data Localization Audit

- Audit of Storage of Payment System Data as per the circular issued by Reserve Bank of India dated April 06, 2018, (https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244) and FAQs on Storage of Payment System Data (https://m.rbi.org.in/scripts/FAQView.aspx?Id=130).

3. Cyber Awareness Training & Phishing Simulation

- Online training to all staff on cyber hygiene, phishing, email safety, data handling.

- Bank-wide phishing simulation and maturity scoring.

- Department-level performance reports and recommendations.

4. Deliverables

-1st Draft Audit Report covering all preliminary findings, observations, and compliance gaps for review by the Bank.

-VAPT Reports (Internal & External) – Two Rounds:

Round 1 – Initial VAPT Report
Round 2 – Retest/Verification Report after remediation

-Network & Security Device Configuration Review Report (firewalls, routers, switches, VPN, WAF, IDS/IPS, AD, endpoints).

-Data Localization Compliance Report as per RBI guidelines.

-Executive Summary for Board / Management highlighting key risks, strengths, gaps, and recommendations.

-Final Audit Report incorporating bank responses, retest results, and closure status of vulnerabilities.

5. Timelines

- Completion of DC, DR, and Branch Audits:
All fieldwork covering the Data Centre (DC), Disaster Recovery Site (DR), Head Office (HO), and all Branches must be completed **within 2 months** from the date of issuance of Work Order.

-Submission of Final Audit Report:
The Final Audit Reportmust be submitted **within 15 days after completion of all fieldwork.**

The Assam Co-op. Apex Bank Ltd. Insp. & Audit. H.O. Guwahati