PEOPLE'S OWN SAVINGS BANK OF ZIMBABWE (POSB)
INVITATION FOR EXPRESSION OF INTEREST

FOR THE PROVISION OF UNIFIED CYBER SECURITY AUDIT CONSULTANCY POSBEOI2026/05

1. BACKGROUND

The People's Own Savings Bank (POSB) is a financial institution committed to maintaining the highest standards of security for its information systems, customer data, and operational integrity. In an increasingly sophisticated cyber threat landscape, regular and independent security audits are critical to identifying vulnerabilities, ensuring compliance with regulatory requirements, and safeguarding our assets.

In this regard, the Bank requires a comprehensive, **Unified Security Posture** assessment proposal from qualified and experienced cybersecurity audit firms that produces both a **current-state baseline** and a **target-state reference architecture** aligned to **Zero Trust** principles and POSB's **AI-enabled orchestration** strategy—spanning on-prem, cloud (IaaS/PaaS/SaaS), applications, data, identity, payments, and third-party fintech integrations. Findings and recommendations must be **mapped to NIST CSF 2.0**, the **RBZ Cybersecurity and Resilience Guideline**, **the Cyber and Data Protection Act [Chapter 12:07]** alongside **Statutory Instrument 155 of 2024**, the **PCI DSS v4.0/4.0.1** for card environments and the **SWIFT CSP/CSCF** for messaging infrastructure.

2. PROJECT OBJECTIVES

The objective is to provide an independent assessment of the bank's current security posture, identify potential weaknesses, and recommend actionable strategies for improvement.

The primary objectives of this unified security audit are to:

- **Assess Current Security Posture:** Evaluate the effectiveness of existing security controls, policies, procedures, and technologies in protecting the Bank's information assets from cyber threats.
- **Identify Risks** Discover technical and administrative risks in systems, applications, networks, and processes that could be exploited by malicious actors.

- **Evaluate Compliance:** Determine the Bank's adherence to relevant industry standards, regulations, and best practices.
- **Provide Actionable Recommendations:** Offer clear, prioritized, and practical recommendations for mitigating identified risks and enhancing the Bank's overall cybersecurity resilience.
- **Enhance Security Awareness:** Contribute to a stronger security culture within the Bank through insights and findings.
- **Provide detailed risk quantification** (FAIR or equivalent) with **costed options** and **expected risk reduction.**;
- **Provide a Zero Trust maturity & rollout plan** (identity, device, network micro-segmentation, app, data, automation).
- **Provide a Detection engineering pack**: MITRE ATT&CK-mapped detection coverage, content backlog for SIEM/SOAR/XDR, and measurable improvements.
- **Provide Resilience validation**: RPO/RTO evidence, ransomware resilience, backup immutability/WORM and regular restore tests.
- **Assess Regulatory Conformance**: RBZ Cybersecurity and Resilience Guideline, CDPA/Chapter 12:07 & **SI 155 of 2024**.

3. SCOPE OF WORK

The scope of this cybersecurity audit shall encompass, but not be limited to, the following key areas:

3.1. Infrastructure & Network Security:

- Network architecture review
- Wireless network security
- Remote access security (VPNs, multi-factor authentication)
- Review core network device configurations and hardening mechanisms.
- Zero Trust network segmentation/Micro-segmentation.

3.2. Application Security:

- Security review for key banking applications (core banking system, internet banking, mobile banking, treasury system, etc.)
- Application development lifecycle security review (SDLC)
- API/Open Banking and mobile apps.

3.3. Server & Endpoint Security:

- Review operating system security (Windows, Linux, Unix)
- Review server hardening and patch management processes
- Review endpoint protection (antivirus/anti-malware, EDR)
- Review configuration management processes
- Review user physical workstation security
- XDR/MDR containment tests
- Review UEM/MDM for corporate/BYOD security
- Review Bastions/jump hosts including for the SWIFT environment
- Review endpoint hardening baselines.

3.4. Data Security & Privacy:

- Review data inventory, data classification and handling procedures
- Encryption at rest and in transit
- Review Data loss prevention (DLP) controls and procedures
- Review database security configurations
- Review access controls to sensitive data

3.5. Identity & Access Management (IAM/IGA/CIEM/PAM):

- Review user provisioning and de-provisioning processes
- Review authentication mechanisms including MFA
- Review authorization controls (least privilege, role-based access control - RBAC)
- Review privileged access management (PAM)
- Identity Lifecycle, SoD, Periodic access reviews.

3.6. Security Operations & Monitoring:

- Review security monitoring & threat intelligence capabilities
- Review Security Information and Event Management (SIEM) effectiveness
- Review Log management and retention across key systems and applications
- Incident response plan (IRP) review Threat hunting cadence
- Review current purple team exercises mapped to MITRE ATT&CK, with coverage metrics and alert fidelity KPIs.

3.7. Policies, Procedures & Governance:

- Review Information security policies
- Security awareness training programs review
- Business continuity planning (BCP) and disaster recovery (DR) review
- Review of fault tolerance tools and infrastructure such as redundancy, load balancing etc for key Bank processes
- Third-party risk management reviews (vendor security assessments)
- Risk management framework review
- Change management processes review
- Three lines of defense clarity and review
- CSF 2.0 governance mapping.
- AI governance policies per NIST AI RMF 1.0.

3.8. Physical Security (limited to IT infrastructure areas):

- Review Data center security controls
- Review Environmental controls (power, cooling, fire suppression)
- Facility resilience checks (N+1 power/cooling, fire suppression type), access logging and review, secure media handling.

3.9 Cloud & SaaS Security (CSPM/SSPM/CIEM)

- Review cloud security configurations against industry best practices and regulatory requirements. Scope may include the following
    - Organisational structure
    - Baselines
    - Misconfiguration controls
    - Shared responsibility
    - Continuous monitoring.

3.10Third-Party/Fintech Orchestration Security

- Review of SBOM in third party applications and systems
- Review security certifications including Pen-test attestations from third parties

  Review SLAs for breach notices, exit plans, continuous ratings, support and maintenance, incident response etc

4. MANDATORY REQUIREMENTS

The following documents shall be considered for shortlisting of Firms

i. Company Profile
ii. Bid Securing Declaration
iii. Certificate of Incorporation for companies, Partnership agreement for Partners and Joint Venture agreement for Joint Ventures or equivalent
iv. Valid PRAZ Registration Certificate under the relevant category
v. NSSA Clearance Certificate
vi. Valid Tax Clearance Certificate
vii. VAT Registration Certificate
viii. Bidders must accompany their expressions of interest with CR6 formerly CR14
ix. Methodology as specified under section 7.3
x. Gantt Chart showing the proposed tasks to be performed and the proposed time intervals
xi. Team Composition and CVs, including roles and responsibilities of each member.
xii. Three Traceable References as specified under Sec. 7.2 below
xiii. Project Management processes and Communication as specified under section 7.4 below
xiv. Quality Assurance processes as specified under Section 7.5 below
xv. Legal and Contractual information as specified under section 7.6

5. DELIVERABLES

The firm selected shall provide the following deliverables:

- **Inception Meeting:** Kick-off meeting with the Bank's relevant stakeholders to confirm scope, methodology, and timelines.
- **Audit Plan:** A detailed audit plan outlining the specific tests, methodologies, timelines, and resources to be deployed.
- **Regular Progress Updates:** Weekly or bi-weekly progress reports to the Bank's Project Manager.
- **Draft Audit Report:** A preliminary report detailing findings, risk ratings, and initial recommendations for review and feedback by the Bank.
- **Presentation of Findings:** A formal presentation of the draft audit report to the Bank's senior management and relevant committees (e.g., Audit Committee, Risk Committee).
- **Final Audit Report:** A comprehensive, professionally written report including:

    - Executive Summary.
    - Detailed Findings and recommendations.
- **Exit Meeting:** Final meeting to discuss the report and the next steps.
- **Post-Audit Support:** Agreed-upon period of support for clarification of findings and recommendations.

6. METHODOLOGY

Bidders should describe their proposed audit methodology in detail, which should include, but not be limited to:

- **Phases of the audit:** Planning, fieldwork, reporting, follow-up.
- **Tools and techniques:** Specific tools to be used for vulnerability scanning, penetration testing, configuration review, code analysis (if applicable), etc.
- **Risk assessment framework:** How findings will be rated based on likelihood and impact.
- **Communication plan:** How the audit team will communicate with Bank staff throughout the engagement.
- **Data handling and confidentiality protocols.**
- **Approach to minimizing disruption** to Bank operations during the audit.
- **Risk quantification**.

6. Gantt Chart

Provide a Gantt chart clearly showing the proposed tasks to be performed and the proposed time intervals

7. PROPOSAL REQUIREMENTS

Proposals must be structured as follows:

7.1. Executive Summary:

- A concise overview of your understanding of the Bank's needs and your proposed solution.

7.2. Firm Profile & Experience:

- Company background, mission, and relevant experience in cybersecurity audits for financial institutions.

- Team composition:
  - Resumes/CVs of key personnel involved in the audit, highlighting relevant certifications (e.g., CISSP, CISM, CISA, OSCP, CEH, CRISC, PNPT, CRTP, ISO27001, ISO 22301, ISO 42001), copies of certificates should be attached.
  - Clearly define the roles and responsibilities of each team member.
- References: Provide at least three (3) traceable client references, preferably from the financial services sector, for similar engagements conducted within the last three years. Include contact names, titles, organizations, and phone numbers/emails.

7.3. Proposed Approach and Methodology:

- Detailed description of your audit methodology as per Section 5.
- Specific scope interpretation and any proposed additions or exclusions with justifications.
- Proposed timeline and work plan with key milestones.
- Resource allocation (number of auditors, their expertise, estimated effort).

7.4. Project Management & Communication:

- Describe your approach to project management for this engagement.
- Outline your communication plan with the Bank.

7.5. Quality Assurance:

- Describe your internal quality assurance processes for audit engagements and report delivery.

7.6. Legal and Contractual Information:

- Proof of business registration and relevant licenses.
- Insurance certificates (e.g., professional liability/errors and omissions, general liability).
- Standard terms and conditions (if available, otherwise the Bank's terms will apply).
- Declaration of any potential conflicts of interest.

8. TECHNICAL EVALUATION CRITERIA

Proposals will be evaluated based on the following criteria:

- **Relevant project experience & Past Performance of the organization in the last 5 years [20%]:** Track record in cybersecurity audits, particularly within the financial sector, and positive client references.
- **Team Qualifications and Expertise [30%]:** Credentials, certifications, and relevant experience of the proposed audit team.
- **Technical Approach & Methodology [25%]:** Clarity, comprehensiveness, and effectiveness of the proposed audit methodology, tools, and work plan.
- **Project Timelines & Milestones [10%]:** Demonstrated ability to manage the project efficiently and communicate effectively and deliver within timelines.
- **Awareness of Local Regulations and Requirements [5%]: Awareness** of the local market context including RBZ guidelines on cybersecurity**.**
- **Quality Assurance and Risk Management [10%]:** Robustness of quality assurance processes and clarity of proposed deliverables.

The Pass mark to the technical evaluation shall be 70%, and bidders who score below this mark shall be eliminated. Only the top six ranked bidders who pass the technical assessment shall be invited to submit firm and final proposals which shall include the financial proposal.

9. FINANCIAL PROPOSALS

Bidders are advised not to submit their financial proposals with this EOI. A Request for Proposals (which includes Financials) shall be sent only to shortlisted bidders requesting for the following:

- Detailed fee proposal, clearly itemized for all services (e.g., daily rates, fixed fee, expenses).
- Breakdown of costs per phase or per area of the audit.
- Proposed payment schedule linked to deliverables.
- Specify any additional costs that may arise.

10. TERMS AND CONDITIONS

- The Bank reserves the right to accept or reject any or all proposals, in whole or in part, without assigning any reason whatsoever.
- The Bank reserves the right to negotiate with one or more Bidders.
- The Bank may request additional information or clarification from Bidders.

- All costs incurred in the preparation and submission of proposals shall be borne by the Bidder.
- Proposals shall remain valid for a period of 90 days from the response deadline.
- The successful Bidder will be required to sign a Non-Disclosure Agreement (NDA) and a Service Level Agreement (SLA) with the Bank.
- The Bank shall not be liable for any claims or damages arising from the cancellation or modification of this RFP.

11. SELECTION PROCEDURE

Consultants will be selected in accordance with the procedures specified in Part VIII of the Public Procurement and Disposal of Public Assets Act [Chapter 22:23] and Part VI of the Public Procurement and Disposal of Public Assets (General) Regulations, 2018 (Statutory Instrument 5 of 2018).

Prequalified firms will subsequently be invited to submit their firm and final proposals, which will include financials on a separate document based on the Request for Proposals (RFP). The firm with the selected proposal will be engaged on the contractual terms set out in that document and in the General Conditions of Contract governing Public Procurement and Disposal of Public Assets Act (Chapter 22:23). Copies of the Act and Regulations and the standard documentation are available on the website of the Procurement Regulatory Authority of Zimbabwe website.

- **The minimum pass score is 70%**
- A maximum of (6) of the highest ranked consultants will be shortlisted for purposes of proceeding with the Request for Proposals (RFP).

Late applications will not be considered, and no liability shall be accepted for loss or late delivery. People's Own Savings Bank (POSB) shall not be responsible for any costs or expenses incurred by firms in connection with preparation or delivery of the application

12. CLARIFICATION

Enquiries and further information relating to the bidding process can be obtained through Electronic Procurement System (egp. https://egp.praz.org.zw) during office hours or may be requested in writing by any bidder before 06 March 2026 and should be sent to procurement@posb.co.zw to the attention of Godfrey Marecha or Gibson Sibanda.

13. BID VALIDITY

Bids must remail valid for a period of 90 days from the date of submission. Bidders are advised to state this in their submissions.

12. SUBMISSION OF PROPOSALS

Expression of Interest documents are available online on the Electronic Government Procurement portal **egp**.

Expression of interest submission must be online through the Electronic Government System (egp.http://egp.praz.org.)zw) not later than the prescribed date.

Late bids will not be considered.

Date of Deadline 13 March 2026 **Deadline time** **1100 Hrs**

Submission Address **Egp.https: egp.praz.org.zw**

Means of Acceptance **Electronically as above**

The bidding submission documents should be scanned as a single document for the relevant slot on eGP

Evaluation Matrix (weighted)

Criteria	Description	Weight (%)	Score	Weighted Score *(Weight x Score)
Relevant project experience & Past Performance of the organization in the last 5 years Cyber Audit [4] ISO27001 [4] SWIFT CSP [2] PCI DSS [2] ISO 22301/ Related Incidence response or Business Continuity Framework[2] Banking Sector Experience [2 for each client up to a maximum of 6]	Experience with similar projects, assessments, client references, and success history.	20%		
Team expertise & sector/regulatory relevance **Team Lead 10%** Security Governance [2] CGEIT/CCISO/CISM Penetration Testing [2] ISO Frameworks [2] PCI DSS Framework [2] CDPO [2] **Up to 3 Consultants 20%** Penetration Testing [4]	Technical depth in security and related frameworks i.e. PCI, SWIFT, Zimbabwe CDPA, Zero-Trust, ISO27001, ISO 22301, ISO 42001. Provide proof of Technical Team Qualifications.	30%		

Criteria	Description	Weight (%)	Score	Weighted Score *(Weight x Score)
ISO 27001 [2] ISO 22301 [2] PCI DSS [4] CDPO [2] NIST Framework [2] Security Certification CISSP, GIAC [2] ISO42001 [2]				
Technical approach & Methodology **Scope coverage and comprehensiveness**	Clarity, comprehensiveness, innovativeness, and feasibility of proposed approach	25%		
Project Timelines & Milestones 8 weeks and below - [10] >8 weeks to 10 weeks – [8] >10 weeks to 12 weeks – [6] >12 weeks – [4]	Realism and clarity of project schedule, milestones, and deliverables	10%		
Awareness of Local Regulations and Requirements	Awareness of CDPA, RBZ guidelines	5%		
Quality Assurance & Risk Management	Bidder's risk management maturity demonstration which may include certifications such as SOC, ISO, PCI or equal.	10%		

Bid-Securing Declaration

{The Bidder must fill in this Form in accordance with the instructions indicated, where it has been stated in the Bidding Procedures that a Bid-Securing Declaration is a requirement of bidding}.

Procurement Reference number:

Date: ……..……*[date (in day, month and year format)]*

Bidder's Reference Number:

To: *{full name of Procuring Entity}*

We, the undersigned, declare that:

We understand that, according to the terms and conditions of your bidding documents, bids must be supported by a Bid Securing Declaration.

We accept that we may be debarred from bidding for any contract with a Procuring Entity in Zimbabwe for a period to be determined by the Authority, if we are in breach of our obligation(s) under the bidding conditions, because:

(a) we have withdrawn our Bid during the period of Bid validity; or

(b) having been notified of the acceptance of our Bid by the Procuring Entity during the period of bid validity, we fail or refuse to execute the Contract.

We understand this Bid Securing Declaration will expire if we are not the successful Bidder, either when we receive your notification to us of the name of the successful Bidder, or twenty-eight days after the expiration of our Bid, whichever is the earlier.

Signed …….. Name: ……

In capacity of: …….. Date: ……(DD/MM/YY) Duly

authorized for and on behalf of:

Company ……

Address: ……

Corporate Seal (where appropriate)