PEOPLE'S OWN SAVINGS BANK OF ZIMBABWE (POSB)

INVITATION TO EXPRESSIONS OF INTEREST

PREQUALIFICATION FOR THE PROVISION OF QUALIFIED SECURITY ASSESSOR (QSA) CONSULTANCY SERVICES LEADING TO THE PCI DSS COMPLIANCE AND CERTIFICATION

PART A. BACKGROUND

The People's Own Savings Bank of Zimbabwe (POSB) invites Expressions of Interest from eligible **Consulting firms** for the provision of Qualified Security Assessor (QSA) Consultancy services leading to the Payment Card Industry Data Security Standard (PCI DSS) Version 4.0.1 compliance and certification of the Bank.

The consultants will be required to assist the bank in every step of the certification process, including scoping, gap analysis, implementation, internal audit and compliance maintenance. The Bank expressly stipulates that the QSA's selection under this Expression of Interest (EOI) is on the understanding that this EOI contains only the principal provisions for the entire assignment and that delivery of the deliverables and the services in connection therewith are only a part of the assignment.

The QSA shall be required to undertake to perform all such tasks, render requisite services and make available such resources as may be required for the successful completion of the entire assignment at no additional cost to the Bank. Consultants may associate with other firms in the form of a joint venture or sub consultancy to enhance their capacity and qualifications.

Consulting firms 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) as amended and in accordance with the shortlisting criteria indicated in the expression of interest (EOI) document. Shortlisted consulting firms will be required to submit their final proposals on a separate document based on a **Request for Proposals (RFP)** for the selection of the consultancy services. Consultants may be requested to explain their proposals before a selection panel. The consultant submitting the successful proposal will be engaged in a contract according to the general conditions of contracts for consultancy services set by the Procurement Regulatory Authority of Zimbabwe. Copies of the Act and Regulations and Standard Documentation are obtainable on the website of the Procurement Regulatory Authority of Zimbabwe.

PART B. ADMINISTRATIONAL CONSIDERATIONS:

The following documentation and evidence will be required in support of the Expression of Interest (EOI)

1. Fully signed expression of interest.
2. Valid NSSA Certificate for the current period, if a local company.
3. Copy of the Certificate of Incorporation.
4. Copy of the CR6 form.
5. Copy of the VAT registration certificate, if local company.
6. Copy of the 2025 ITF 263 Tax Clearance Certificate, if local company
7. Detailed Company Profile. The consultants should include an organizational structure indicating the available key personnel, their qualifications should be attached as part of the submission.
8. Proof of registration with PRAZ.
9. Provide qualifications and competences for the team leader and consultants tasked with providing all Key Results Areas.
10. Provide a plan showing the input of all key staff and a clear Gantt chart showing the periods of how long each process will take.
11. The bidder must be enlisted with the PCI council as a QSA and ASV (provide necessary proof).
12. Provide qualifications and competencies for the team leader and assessors tasked with providing the QSA Services. Include CVs detailing qualifications and copies of certificates, relevant experience, and necessary domain knowledge.
13. Provide a detailed methodology for performing the QSA Services.

14. Provide the firm's track record and experience in conducting similar assignments. Submit documentary evidence describing relevant assignments, experience in similar conditions, and staff skills availability. Include a minimum of 3 reference letters with contact information from reputable organizations conducted within the last 5 years. The sites may be visited during the evaluation process as part of due diligence.
15. Bidders should not be under debarment/blacklist for breach of contract/fraud/corrupt practices on the date of submission of bid for this EOI.
16. The Bidder should have the following as permanent roles, and this should be clearly stated in the proposal.

- PCI Qualified Security Assessors (QSAs)
- Payment Card Industry Professional (PCIP)
- PCI 3DS Assessor
- CISA certified personnel
- CISSP certified personnel
- CISM certified person

FAILURE TO ABIDE BY ANY OF THE ABOVE REQUIREMENTS MAY LEAD TO AUTOMATIC DISQUALIFICATION

As part of due diligence: -

- The People's Own Savings Bank of Zimbabwe (POSB) may contact referees of referred projects/clients and /or visit the cited works and bidders' premises as part of the evaluation exercise.
- POSB may invite consultants for interviews or demonstrations of their proposals, capacity, profiles and appreciation of the consultant's understanding of the bank's requirements.

PART C. TERMS OF REFERENCE/SCOPE OF WORK

NO	REQUIREMENTS	COMMENTS
1	Description of Services	Provide services of Qualified Security Assessor for PCI DSS Certification.
2	Description of deliverables	See Description of Services and Deliverables below.

3	Security Requirements	Bidder to adhere to Bank's information security policies and procedures in conducting audit/activities listed under this RFP.

Description of Services and Deliverables

Below is the list of activities to be performed by Bidder for certification. Any activity performed once during the tenure of the contract does not imply that the same need not be performed and the same needs to be performed by the Bidder unless compliant.

Phase 1: Scope Identification & Evaluation

This phase involves **identification** of:

- Assets/ Locations/ Technologies/ Process/ Service Providers/ Infrastructure (including shared infrastructure) components involved in Card Holder Data (CHD) processing.
- Locations, departments, and teams involved in CHD processing.
- Business processes involved CHD processing at each location of the Bank.
- Delivery channels for the identified CHD processes.
- Applications, processes, functions, and other systems with respect to the business processes involved in CHD processing.
- Services rendered by POSB for the identified CHD process.
- Service providers' access to POSB's CHD environment.
- Places where there is remote access to the card holder data environment.

This phase involves **analysis and evaluation** of:

- Network segments implemented for the systems and processes under scope.
- Existing security guidelines of the Bank regarding policy, organization, personnel, physical control, network management etc.
- All pre-requisite software, hardware and any other requirement for compliance.
- PCI DSS scope for the Bank such that all critical assets are covered without compromising any security.
- IP addresses required for internal vulnerability assessment and internal penetration testing limited to the scope of audit.
- Applications required for internal application penetration testing.
- IP addresses required for external vulnerability scan by Approved Scanner Vendor (ASV) limited to the scope of audit.
- Applications required for external application penetration testing.
- IP addresses required for external network penetration testing.

- Segments/VLANs to be considered CDE In-Scope, Non-CDE In-Scope and Out of Scope for segmentation penetration testing.
- Connected entities with the environment in-scope.

This phase will involve **creation and documentation** of:

- Service providers involved in the identified CHD process.
- Information shared with service providers for the identified CHD processes.
- Asset inventory covering all the assets in scope including shared infrastructure with detail documentation of the applications, databases, servers, desktops, laptops, network and security devices, media and other system components that are part of Card Data Environment (CDE).
- High Level and Low-Level Data Flow Diagram.
- High Level and Low-Level Network/Architecture Diagram.
- Process flow documents for each identified process.
- Policies/procedures/any other document(s)/diagrams/flows required for PCI DSS certification.
- Card Data Matrix duly incorporating details such as Location, System Name, Application, Data Store, Type of CHD, Reason for Storage, Retention Period, Auditing Mechanism, Protection Mechanism, Secure Deletion Mechanism, Application Log Location and any other important details limited to the scope of audit.

Deliverables of Phase 1 to be provided by Bidder:

1. Asset inventory (as per PCI DSS Scope).
2. VLAN List with CDE In-Scope, Non-CDE In-Scope and Out of Scope VLANs for Segmentation Penetration Testing.
3. Card Data Matrix
4. High Level and Low-Level Data Flow Diagram
5. High Level and Low-Level Network/Architecture Diagram
6. List of connected entities
7. List of assets (including shared infrastructure, if applicable) for:
    a. Internal Vulnerability Assessment and Penetration Testing
    b. External Network Penetration Testing
    c. Approved Scanning Vendor (ASV) Scan
8. List of applications (including shared infrastructure, if applicable) for:
    a. Internal Application Penetration Testing
    b. External Application Penetration Testing
9. Schedule of activities along with Pre-requisites for the activities.

Note*: All the documents above need to be updated by the bidder on an ongoing basis as and when needed, across all phases as listed in this document.

Phase 2: Gap Assessment

- Conduct Gap Assessment, of applications, processes, infrastructure systems and other system components that are part of the scope and report gap areas with detailed remediation actions.
- Perform a review of security solutions such as antivirus solutions, encryption, FIM, DLP, IAM and other solutions applicable for the in-scope systems, applications, and interfaces.
- Report on Gap Assessment.
- Report initial compliance level and remediation action plan roadmap and final compliance.

Deliverables of Phase 2 to be provided by Bidder:

1. Documented results of the Gap analysis clearly showing compliant and noncompliant items.
2. Ordered plan for addressing findings with highest risk exposure on priority basis.
3. Document and provide clear recommendations for the remediation and closure of the gaps identified.
4. List of software/hardware to be procured by the Bank to be in compliance.

Phase 3: Gap Remediation/Mitigation Support/Evidence Collection

- The bidder is required to keep liaison with the stakeholder departments and conduct meetings to formulate Gap remediation plan and alternative compensatory controls.
- The bidder is required to help the Bank using their technical expertise to identify the products and services to be procured from vendors to meet the PCI DSS requirements. Further, the bidder shall extend support in evaluating the vendor products.
- The bidder shall extend **hand-holding support** with respect to closure of all the gaps or suggesting alternate methods of risk mitigation adhering to PCI DSS standards.

- Conduct pre-audit assessment for all in-scope components and submit detailed report after the remediation.

Deliverables of Phase 3 to be provided by Bidder:

1. Report of Pre-Audit with compliance status reports highlighting non-compliant findings with detailed recommendations to close the corresponding gap items.
2. Provide detailed implementable remediation actions for each of PCI DSS requirements and corresponding non-compliant items (applications, servers and related system components)

Phase 4 Final Audit & Certification

- The bidder is required to perform audit planning, open meetings with key stake holders, identifying sampling approaches, perform validations & conformation on PCI DSS.
- The bidder is required to perform verification of individual control requirements for in-scope applications, processes, and other system components (including shared infrastructure) & perform QSA audit and submit reports on compliance.
- Detailed remediation actions for each of non-compliant applications, servers, and related system components, if any

Deliverables of Phase 4 to be provided by Bidder:

1. Final "Report on compliance" (ROC) for PCI DSS compliance along with "Attestation of Compliance (AOC)" and "Certificate of Compliance (COC)".

Phase 5: Post- Certification ongoing compliance

- Perform activities as required from phase 1 to 4 in scope of work to meet ongoing compliance.
- The QSA must conduct periodic meetings with the Bank to ensure that the post-certification compliance requirements are met by the Bank. The QSA will have to consult the Bank and advise in case of any gap found.
- QSA will alert the Bank of any potential threat/zero-day attack impacting the payment card infrastructure anywhere in the world.
- QSA must design, update and maintain PCI DSS compliant documentation template whenever required
- QSA must provide support for verifying compliance of PCI-DSS for changes in system and evaluating and designing detailed compensating controls wherever required.

Deliverable of Phase 5 to be provided by Bidder:

1. Scan report for ASV, VA, PT as required by the standard
2. Report on compliance
3. Attestation of compliance

4. Certificate of compliance

Miscellaneous Terms:

1. The selected bidder/QSA shall be required to independently arrive at Methodology and Approach, based on PCI-DSS requirements and best practices, suitable for the Bank, after taking into consideration the effort estimate for completion of the same.
2. The QSA must track the PCI DSS project progress and periodically report to management.
3. The QSA should give a clear Gantt chart showing how long each process will take to effectively have all proposed steps properly executed.
4. The agreement with the QSA will be applicable for period of 3 years which includes the first-year certification process, and subsequent two years recertification as per the latest requirements of PCI DSS. After the above Contract Period, the Bank may at its discretion, extend the contract for another term of 3 years at the negotiated cost, with the vendor.

Technical Evaluation Criteria

Sr. No.	Evaluation Matrix	Max Marks	Supporting Evidence to be submitted
1.	Bidder's Years of Experience as a QSA for PCI DSS. Up to 3 (6 marks) Greater than 3 but less than 5 years (15 marks) Greater than 5 years up to 6 max (20 marks)	20	1. Letter from PCI Council highlighting years of experience as QSA **OR** 2. Letter from Bidder on its letterhead confirming their years of experience.

Sr. No.	Evaluation Matrix	Max Marks	Supporting Evidence to be submitted
2.	Number of PCI DSS Certification/Recertification Projects completed for Banks or Payment Gateway/ Payment Processors/Core Banking during the last 5 calendar years. Up to 2. (6 marks) Greater than 2 but less than 4. (12) marks) Greater than 4 up to 6 max. (21) Southern Africa Based Client (Extra 2 points for each up to a max of 4)	25	1.i) Provide Certificate of Completion for each client. **OR** 1.ii) Provide a letter on the bidder's letterhead confirming list of clients and date of completion of their respective PCI DSS certification along with contact details of client. **AND** 2.) Client reference -The bank reserves the right to carry out independent verifications including site visits where necessary.
3.	Number of PCI-QSA certified employees with the bidder on its own payroll. Up to 2. (6 marks) Greater than 2 but less than 4. (8 marks) Greater than 4. (15 marks)	15	1.) Valid QSA certificate of each employee **AND** 2.) Employment proof in the form of employment letter or suitable declaration jointly signed by the Employer and Employee
4.	Number of CISA/CISSP/CISM/ certified employees with the bidder on its own payroll. Up to 2. 5 marks) Greater than 2 but less than 4. (8 marks) Greater than 4. (15 marks)	15	Valid certificate of each employee.
5.	The quality of the methodology proposed and accommodation of scope including risk management and quality assurance Scope Coverage (5 Marks) Risk Management (5 Marks) Quality Assurance (5 Marks)	15	Scope Coverage & Methodology Demonstration of in depth understanding of the Bank's project requirements through the technical proposal and presentation, with detailed broken-down activities to be performed, effort estimation and manpower to be deployed.

Sr. No.	Evaluation Matrix	Max Marks	Supporting Evidence to be submitted
6.	Delivery Period maximum [36 Weeks] Less than or equal to 36 weeks (10 marks) Greater than 30. (0 mark)	10	Workplan & Gant Chart

- **The minimum technical pass score is 80%.**
- **A maximum of six (6) consulting firms will be shortlisted and will be requested to submit detailed technical and financial proposals for final selection.**

PART D. EXPRESSION OF INTEREST DOCUMENT AND SUBMISSION OF PROPOSALS

Expression of interest documents are available online on the Electronic Government Procurement Portal **eGP**

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

Enquiries and further information relating to the bidding process can be obtained through Electronic Government Procurement System **(eGP.https://egp.praz.org.zw**) during office hours.

Date of deadline: - **11 April 2025** **Deadline Time 10.00 Hours**

Submission Address: - **eGP.https://egp.praz.org.zw**

Means of acceptance: - **Electronically as above.**