Terms of reference for the Provision of PCI DSS gap assessment Services

Background

KCB Group Plc is the largest bank in Eastern and Central Africa, commanding the largest banking network in Eastern Africa and as a player in the global financial market, maintains working arrangements with correspondent banks throughout the world. KCB Group Plc consists of several subsidiary companies operating in Kenya, Tanzania, Uganda, South Sudan, Rwanda, Burundi and DRC with the Head Office located in Nairobi, Kenya.

KCB Bank Group is both an issuer of debit and credit cards and an acquirer providing merchant services. In 2023, KCB Kenya footprint for Agency outlets was 17,504, POS/Merchant outlets 6,276 and ATMs 477. The value of transactions done through agency banking had a 122% increase between 2019 and 2023 while for merchant POS the value increases by 334%. Both services are run using POS machines that are under scope for PCI DSS.

Additionally, in the last strategic cycle the bank launched various offerings in the card space including MasterCard World Elite, Visa Infinite and Signature cards. Other services launched included the tap phone to pay for cardholders to make card payments using mobile phones and tap to phone card acceptance solution for MSMEs. More recently in 2024, the bank launched a multicurrency prepaid card.

The bank is looking to establish a partnership with a PCI Qualified Security Assessor to assist with a gap analysis, review and development of required internal policies and documents where required, all validation, testing and assessment requirements towards compliance with the Payment Card Industry Data Security Standards services.

1.1. Aims and Objectives

The consultant will be responsible to deliver the following objectives:

- **Gap Analysis & Readiness Assessment:** Evaluate the current card ecosystem, identify gaps and recommend improvements.
- **Policy & Process Development:** Assist in developing and aligning policies, procedures and documentation with PCI DSS latest version
- **Training & Awareness:** Conduct training for key stakeholders on PCI DSS standards and best practices.
- **Remediation Support:** Guide key stakeholders in adopting necessary process changes and improvements.

1.2. Scope of Work

The Bank is requesting proposals from qualified information security and compliance service firms to provide PCI DSS consultancy services towards achieving the following.

1. **Onsite PCI Gap Assessment -** Accurately evaluate the card ecosystem security processes and controls consistent with applicable PCI DSS requirements and testing procedures. These include but are not limited to;
   - Card & Payment operational processes,
   - Card & Payment processing systems,
   - Payment processing infrastructure,
   - Cybersecurity Architecture in relation to PCI DSS compliance,
   - Documentation reviews,
   - PCI ASV Scan Services & External Penetration Testing
   - Internal VA & Penetration Testing
   - Third party card flow reviews etc.
   - Deliver an initial gap assessment and recommendations for improvements as per PCI DSS latest version.
2. **Gap Remediation Support & Guidance**
   - Provide roadmap for developing and implementing controls to address the identified gaps.
   - Support on updating the Policies & Procedures Documents as per PCI DSS latest version
   - Certification readiness checklist & guidelines for meeting compliance.
3. **Training**
   - Conduct targeted PCI DSS training for key personnel
   - Facilitate awareness workshops for relevant personnel.

The selected bidder/QSA is required to provide clear guidance towards PCI-DSS compliance and eventual certification for KCB Group.

1.3. Deliverables

The vendor should provide a proposal covering the approach and methodology for delivery of the following:

Phase 1: Gap Assessment

- Details of the environment for which GAP assessment is to be carried out
- Gap assessment report with recommendations
- Vulnerability scan and penetration testing report

Phase 2: Gap Remediation

- Gap remediation plan
- Modified or recommended security policies, procedures, processes and architectural designs.
- Technical support & assistance for remediation of gaps to meet PCI-DSS requirements.
- Training for the target group of personnel handling payment card data including materials & presentations.

Phase 3: Certification readiness

- Checklist for ensuring ongoing compliance
- Procedural guidelines for meeting ongoing compliance
- ASV scan, VA, PT reports and other scan reports.

2. Technical Requirements

The Technical proposal should demonstrate the following:

- The vendor must be certified/qualified to perform assessments as required by PCI DSS validation requirements for qualified security assessors.
- The vendor should have at least five years' experience in performing PCI DSS and related assessments/consulting in an organization of the same or larger size as KCB Bank.
- The bidder should have provided information/cyber security consultancy/VA/PT and QSA services to minimum two institutions the size of KCB during last 3 years from the date of RFP.
- The bidder must have satisfactory experience of at least 3 years of providing Audit or PCI-DSS certification services to at least two Financial Institutions/Banks.
- The bidder should confirm how often the certified PCI Assessors are required to attend training to keep them appraised of all current PCI regulations.
- The bidder must have at least 2 full-time technically qualified personnel with certifications like ISO 27000/CEH/CISA/CISSP and on its payroll in Information technology specifically in the areas of IT Audit/Data Centre Audit/Banking Audit, IT Security etc. as on date of bid submission.
- The Bidder must be a QSA certified by PCI-SSC for the past 5 years.
- The vendor must provide evidence of certification: Provide the number of trained and certified PCI Assessors that will be conducting the assessment.
- The bidder must be enlisted with the PCI council as a QSA and ASV
- Must remain certified and be listed on the PCI Security Standards Council website and listed as such for the period the Firm is engaged with KCB Bank.

3. Overall Responsibility

a) The Bidder is obliged to work closely with the KCB team, act within its own authority, and abide by directives issued by the Bank that are consistent with the terms of the Contract.

b) The Bidder will abide by the job safety measures and will indemnify the Bank and its related third parties from all demands or responsibilities arising from accidents or loss of life, the cause of which is the Bidder's negligence. The Bidder will pay all indemnities arising from such incidents and will not hold the Bank responsible or obligated.

c) The Bidder is responsible for managing the activities of its personnel, or subcontracted personnel, and will hold itself responsible for any misdemeanors.

d) The Bidder shall appoint an experienced counterpart resource to handle this requirement for the duration of the Contract. The Bank may also demand a replacement of the Project lead if it is not satisfied with the Project Lead's work or for any other reason.

e) The Bidder shall take the lead role and be jointly responsible with the project for producing a finalized project plan and schedule, including identification of all major milestones and specific resources that the Bank is required to provide.

f) The Bidder shall not disclose the information it has access to, during the course of the Consultancy, to any other third parties without the prior written authorization of the Bank. This clause shall survive the expiry or earlier termination of the contract.

3.1. Pricing / FINANCIAL PROPOSAL

Provide your financial proposal as per the table below.

No.	Activity	Cost (Ksh)
1	PCI DSS scoping and Onsite Gap Assessment	
2	Gap Remediation	
3	PCI DSS training	
	Total Cost (net of taxes)	

The Costs should be in Kenya shillings inclusive of all taxes; clearly stating Man/Day rates where appropriate.

All taxes and VAT must be clearly stipulated and separated from the base costs and should be valid for a minimum of 90 days.

3.2. Delivery

Delivery and performance of the Services shall be made by the successful Bidder in accordance with the time schedule as per Proposal and subsequent Agreement.

3.3. Delayed Delivery by The Consultant

If at any time during the performance of the Contract, the Bidder should encounter conditions impeding timely delivery and performance of the Services, the Bidder shall promptly notify in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the Bidder's notice, shall evaluate the situation and may at its discretion extend the Bidder's time for performance, with or without liquidated damages, in which case the extension shall be ratified by the parties by amendment of the Contract.

3.4. Bid Effectiveness

It is a condition of the Bank that the supplier guarantees the sufficiency and effectiveness of the consultancy proposed to meet the Bank's requirements as outlined in this document. The Bank will hold the supplier solely responsible for the accuracy and completeness of information supplied in response to this tender. The Bank will hold the supplier responsible for the completeness of the consultancy proposed

and that if they were the supplier to be awarded the tender, they would implement the consultancy without any additional requirements from the Bank.

3.5. Payment Terms

The Bank will NOT make any payments in advance. The Bank will issue an LPO for all the services ordered. The LPO will be paid within 45 days after successful delivery, and acceptance of the services being rendered.

The Bank will not accept partial deliveries, and neither will the Bank make partial payments. Payment for services will only be made once the full scope of service has been successfully provided.

NOTE: KCB GROUP PLC SHALL ONLY MAKE PAYMENTS THROUGH A KCB ACCOUNT.

3.6. Responsibility as an Independent Contractor

The supplier agrees to take overall responsibility for any services rendered; regardless of whether third parties are engaged by the supplier, or the supplier himself carries them out.

Submission Criteria

The proposal should be submitted on the KCB Sourcing portal, not later than **Friday 20th June 2015 by 3: 00pm.EAT.** All clarifications to this RFP should be sent to the KCB Sourcing Portal under the messaging section before **Wednesday 18th June 2025**