RFP#111102026-1

TERMS OF REFERENCE (TORs) FOR PROVISIONING OF CONSULTANCY SERVICES FOR PAYMENT CARD INDUSTRY ("PCI") AND DATA SECURITY STANDARDS ("DSS")

1. OBJECTIVE:

Punjab Information Technology Board has previously undergone assessment against applicable requirements of the Payment Card Industry Data Security Standard (PCI DSS) as part of its commitment to maintaining a robust information security and payment security environment.

PITB is again seeking qualified service providers ("Respondents") to provide professional consulting services related to ongoing payment card industry data security standards ("PCI DSS") and payment application data security standards ("PA DSS"): PCI compliance services performed by a qualified security assessor ("QSA"), ("QSA Compliance Services") for Automatic Fare Collection(AFC) Software developed by PITB, in accordance with the requirements defined throughout this RFP. PITB is issuing this RFP to award a contract to a qualified PCI service provider ("Contractor"), thereby allowing for review the developed AFC software and other associated applications and thereby issue PCI-DSS compliance certificate to cater open loop payments in Punjab.

The primary objectives of this assessment are to:

- Review the AFC software and other associated applications and Identify strengths, weaknesses, and areas for improvement.
- Issue PCI Compliance certificates against the AFC software and other associated applications to perform open loop payments.

2. SCOPE OF WORK & EXPECTED OUTPUTS:

The scope of this assessment includes, but is not limited to, the following areas:

2.1 Scope Section 1:

1. PCI DSS Scoping (PITB Arfa Tower Data Centre and DR Site)
2. PCI DSS Gap Analysis over the latest version of PCI at the time of assessment i.e. v4.0.1 and above (whichever is applicable).

2.2 Scope Section 2:

1. Quarterly ASV scans
2. Internet Vulnerability Assessment of Card Data Environment (CDE) (IPs)
3. Internal & External Penetration Testing of Card Data Environment (IPs)
4. Remediation will be done by PITB.

2.3 Scope Section 3:

1. Certification Audit by QSA
2. Report on Compliance (ROC)
3. Attestation of Compliance (AOC) (PCI DSS Certification on latest version)

3. EXPECTED OUTPUTS of PCI DSS:

The consultant firm is expected to provide the following deliverables:

1. Scoping Document
2. Gap Assessment Report
3. Remediation Tracker/Plan
4. Internal Vulnerability Assessment and Penetration Testing (VAPT) Report of Card Data Environment (CDE).
5. Approved Scanning Vendor (ASV) Scan Report.
6. Report on Compliance (ROC)
7. Attestation of Compliance (AOC)
8. PCI DSS Certificate

4. DETAILED REQUIREMENTS of PCI DSS

This section lists the detailed requirements of the undertaking:

4.1 Project Plan: The selected bidder will devise a project plan leading to renewal of PCI DSS certification. The project will be decomposed into several Project Phases with responsibilities of PITB stakeholders defined. Timelines will be reviewed and revisited periodically.

4.2 Scoping: In-depth scoping analysis for PITB's Card Holder Data and Card Holder Environment, technology environment, its supporting components and functions, physical sites and outsourced arrangements. Analyze them to optimize the scope. PCI QSA Must lead the project execution onsite with its team.

4.3 Gap Assessment: For in-scope areas and components as related to the latest version of PCI DSS criteria and its core areas Review and analysis of:

a. Current policies, procedures, and initiatives throughout the organization for meeting PCI DSS compliance.
b. Analysis of payment card holder environment and Card Holder Data environment.
c. Analysis of hardware/software systems, components and all other related application and network layer devices.
d. Identifying and analyzing all significant third-party service providers and suppliers and managed service providers

4.4 Quarterly ASV Scans: For Public facing IPs vendor must conduct scans via Authorized Scanning Vendor (ASV) Tool. Re Assessment for each scan will be a part till compliance is achieved. The documents must be submitted about the company performing ASV Scans, if these services are outsourced.

4.5 Annual Internal & External Penetration Testing via Licensed Penetration Tester or Offensive Security Certified Professional (OSCP) certified resource on public facing CDE Environment of PITB.

4.6 PCI Certification Audit by QSA:

The bidder PCI QSA will perform final assessments as per PCI Security Standard Council (SSC) requirement for all PITB in scope components. It will, at least, cover:

- Review of policies and procedures
- Review of applications and databases configuration
- Review of security devices and controls
- Review of security devices configuration
- Review of business processes
- Interviews of relevant individuals

- Review of datacenter
- Review of necessary in scope assets as per PCI SSC procedure for PCI DSS Audit

4.7 ROC & Compliance documentation

- To finalize ROC
- Submission of ROC for review
- Final Report on Compliance

4.8 Attestation of Compliance (AOC)

4.9 PCI DSS Certificate

5. DELIVERABLES of PCI DSS

1. Scoping Document
2. Gap Assessment Report
3. ASV Scan Reports
4. Internal & External Penetration Testing Report.
5. ROC
6. AOC
7. PCI DSS Certificate

6. DURATION OF THE CONTRACT

The duration of the contract shall be for the period of thirty six months from the date of the issuance of work order, till the issuance of PCI-DSS certification, completion of subsequent ASV Scans and issuance of AOC and ROC reports of PCI DSS.

7. EXECUTION SCHEDULE

The Consultant shall complete the consultancy / provide complete deliverables as per scope of work & expected outputs, within twelve (12) months from the issuance of intimation letter / email by concerned team against each year, after issuance of Work Order and the subsequent quarterly ASV scans will be performed for 3 years after the issuance of PCI certificate.

8. ESTIMATED COST

The total cost estimation for the consultancy for 3 years is PKR Sixty-Five lacs (6.5 Million) inclusive of all taxes.

9. LIQUIDATED DAMAGES

If the Consultant fails / delays in performance of any of the obligations, under the work order / violates any of the provisions of the work order / commits breach of any of the terms and conditions of the work order, the Purchaser may, without prejudice to any other right of action / remedy it may have, deduct from the work order Price, as liquidated damages, a sum of money @0.25% of the total work order Price which is attributable to such part of the Services / the Works, in consequence of the failure / delay, be put to the intended use, for every day between the scheduled delivery date(s), with any extension of time thereof granted by the Purchaser, and the actual delivery date(s). Provided that the amount deducted shall not exceed, in the aggregate, 10% of the work order Price.

10. PROPOSAL EVALUATION CRITERIA

Evaluation of the firms shall be based on information provided in the Proposals. The bidder must obtain 65 marks out of the 100 marks in order to eligible for the opening of financial bids.

11. CRITERIA FOR SELECTION

Only consultant firms meeting the following technical evaluation criteria would be considered for financial evaluation. The bidding document shall be rejected if the vendor fails to meet the following minimum criteria and submission of required documents:

Category	Description	Points
Legal (Mandatory)	Certificate of Company/Firm Registration / Incorporation under the laws of Pakistan. The company must be in business for 5 years. Documentary evidence must be provided.	Mandatory
	Bidder must be a PCI QSA firm. Documentary evidence must be provided.	
	Income Tax Registration Certificate for at least 5 years in business in Pakistan. Documentary evidence must be provided.	
	Valid Sales Tax Registration (Status = Active with relevant authority) Documentary evidence must be provided.	
	Single undertaking covering the following aspects: i. Bidder should provide an undertaking on legal stamp paper/letter head of the firm stating that "The firm is not blacklisted by the procuring agency and PPRA. (ii) The documents/photocopies provided by the firm with its Bid are authentic. (In case of any fake/bogus document found at any stage of the procurement process, the firm shall be black listed as per Rules / Laws.)." ii. Compliance with the scope of services mentioned under TORs of this document. iii. In full compliance of the Execution Schedule and Delivery Period mentioned in this document.	Mandatory
Human Resource	Bidder must have a local PCI QSA in Pakistan who will lead the project onsite– Proof of a QSA in Pakistan to be provided in the shape of CNIC and QSA Certificate.	Mandatory

12. SORTING CRITERIA

Bidder firms who meet the mandatory criteria will be evaluated on following criteria. Technical score (St) of the firms shall be calculated based on following criteria:

Key Characteristics		Max Marks	Remarks
I. Experience of firm		**30**	
1.	Bidder should have completed PCI DSS Certification projects in Commercial Banks/Payment Service Provider/Payment Service Operator or any related organizations. (01 to 02) Assignment =5 (03 to 04) Assignments =7 05 + Assignments = 13	20	Please provide the necessary documentary evidence.

2.	Bidder must be in the information security consultancy services as follows; (01 to 2) Years of experience = 5 points (03 to 4) Years of experience = 7 points 05+ Years of experience = 10 points	10	Please provide the necessary documentary evidence.

II. Work Plan & Methodology for PCI DSS		**20**	
a.	Details related to work plan and methodology that would be used to conduct Scoping. Scoping template to be provided for reference.	8	Detailed Scoping Methodology along with Report Template
b.	Details related to work plan and methodology that would be used for Gap Assessment and Remediation Plan	8	Detailed plan along with timelines to be submitted
c.	Approach and Methodology for PCI DSS Certification Audit	4	Reporting document to be submitted
III. Project Professional Team			
Team Lead as QSA		**20**	
a.	Team Lead must be a QSA and a resident of Pakistan. Certification in PCI QSA will carry 3 Points. Certification in PCI SSF QSA area will carry 3 marks. Resident of Pakistan Evidence 2 marks	8	Detailed CVs on bidder's letter head with copies of testimonials along with Copies of certificates
b.	Certified QSA with Experience of PCI-DSS Assessments, reviews and assisting Banks/Payment Service Provider/Payment Service Operator or any related organizations in Pakistan for compliance certification. Each assignment as QSA will carry 3 Marks	12	Please provide the necessary documentary evidence.
Team Members		**10**	
a.	Bidder must have at least 4 PCI experts in their team having experience of PCI DSS assessments in Pakistan institutions. CVs should be provided for 4 resources who will be involved in the project. Each resource carries 2 marks, max 8 Marks.	8	Detailed CVs on bidder's letter head with copies of testimonials along with Copies of certificates
b.	Bidder must have one qualified OSCP resource for VAPT scans.	2	Please provide the necessary documentary evidence.
Audited Profit & Loss (Income Statement)		**20**	
(Income Statement) showing average sale volume of company of at least Rs. 10 million in the last 2 years. PKR 10-15 million= 10 Marks PKR 15 million or above=20 Marks		20	Please provide the necessary documentary evidence.
TOTAL Marks		**100**	

Note: Passing Marks= 65

Note: Submission of verifiable documentary proof for all above requirements and criteria points are mandatory requirement, and marks will be awarded on the basis of these verifiable proofs. Every document to be duly signed and stamped by the authorized representative of the company.

13. SCOPE OF FINANCIAL PROPOSAL AND PAYMENT SCHEDULE

Financial proposals of consultants fulfilling the above evaluation criteria will be considered for financial evaluation and the consultant will be selected on least cost selection method as per PPRA Rules, 2014.

Payment will be made after completion of consultancy services. The consultancy firm will submit financial proposals in the following format:

Sr. #	Description	(A)	(B)	(C)
		QTY	Unit Cost (incl. all taxes) PKR	Total Cost (incl. all taxes) PKR
1	Consultancy Services for payment card industry ("PCI") and data security standards ("DSS") audit and compliance service including issuance of AOC, ROC, and PCI certificate complete in all aspects as mentioned in the Deliverables	1		**X**

14. PROPOSAL SUBMISSION

The firms are required to submit proposals in a single package consisting of two separate envelopes, containing separately the technical and financial proposals, the envelopes shall be marked as "Technical Proposal" and "Financial Proposal." In the first instance, the "Technical Proposal" shall be opened and the envelope marked as "Financial Proposal" shall be retained unopened in the custody of the procuring agency and subsequently, the financial proposals of technically qualified consultants will be opened and considered for financial evaluation.

Technical and Financial Separate Proposals, duly completed, signed, stamped, and in complete conformity with TOR Document must be Submitted at PITB till **1100 hours on 30th November, 2026** and proposals shall be opened at **1130 hours on the same date**, as per PPRA Rules, 2014.

15. FORMAT OF TECHNICAL BID

The bidders are requested to submit the technical proposal, which at least shall include the following sections

a. Executive Summary
b. Company Profile
c. Proposed Consultancy Services and Approach
d. Project Management Approach
e. Deliverables
f. Timelines
g. Technical Team Composition with Certificates
h. Annexure - Evidences
i. PST/NTN Certificate
j. Company Incorporation Certificate
k. Similar Assignments and References as per eligibility Criteria (Local & International)
l. Team Certificates
m. Audited Statement (Profit and Loss, Balance Sheet, and Cash Flow Statements)

n. PCI QSA enlisted for Pakistan market evidence to be provided.

16. PAYMENT TERMS

- Invoices shall be cleared upon receiving the invoice along with necessary documentation and project milestones. Incomplete claims shall be returned to the vendor.
- Payment processing time shall be 30 days after receiving of Invoice and necessary documentation.
- Taxes shall be deducted at source as per government rules at the time of payment.

Payment Schedule

The following Payment plan will be followed for each year for 3 years respectively:

Project Phase	Payment Plan (% age of Contract Value)
Scoping & Gap Assessment Report of PCI DSS and Assessment Scope Document of PCI SLC	20%
Remediation Plan, Penetration Testing Report of PCI DSS and Assessment Plan, Evidence Request List and Gap Assessment / Preliminary Findings of PCI SLC	30%
Submission of ROC, AOC and PCI DSS Certification and Final PCI Secure SLC Report on Compliance (ROC) and Attestation of Compliance (AOC)	40%
Completion of ASV Scans (four number of scans)	10%

Glossary

- PCI DSS – Payment Card Industry Data Security Standard: A global standard ensuring secure handling of cardholder data by organizations that store, process, or transmit such data
- PA DSS – Payment Application Data Security Standard: A standard for software vendors to ensure their payment applications support PCI DSS compliance.
- PCI DSS v4.0 – The latest version of the PCI DSS, introducing enhanced requirements and flexibility in achieving compliance.
- ROC – Report on Compliance: A detailed report produced by a Qualified Security Assessor (QSA) documenting an entity's adherence to PCI DSS requirements.
- AOC – Attestation of Compliance: A formal declaration by an organization, confirming its compliance with PCI DSS, often accompanying the ROC.
- QSA – Qualified Security Assessor: An individual certified by the PCI Security Standards Council to assess and validate an organization's PCI DSS compliance.
- ASV – Approved Scanning Vendor: An organization authorized by the PCI Security Standards Council to conduct external vulnerability scanning services.
- ISA – Internal Security Assessor: An individual within an organization trained and certified to perform PCI DSS self-assessments.
- CDE – Cardholder Data Environment: The network and systems that store, process, or transmit cardholder data.
- VAPT – Vulnerability Assessment and Penetration Testing: Security testing processes to identify and exploit vulnerabilities in systems.
- ASV Scan – Approved Scanning Vendor Scan: External vulnerability scans conducted by an ASV to identify security weaknesses.
- SAQ – Self-Assessment Questionnaire: A tool for organizations to assess their PCI DSS compliance status.