

THE BANK OF KHYBER

Expression of Interest (EOI)

**SERVICES FOR AUDIT AND SECURITY ASSESSMENT OF
STRAIGHT THROUGH PROCESSING (STP) WITH PRISM-RTGS**

Last Date for Submission:	09-05-2019 at 3:30PM
Opening Date:	09-05-2019 at 4:00PM

Description of Work

A. Introduction

In accordance with SBP's PSD Circular No. 2 of 2016 dated Jan 19, 2016 regarding "Implementation of Straight Through Processing (STP) with PRISM-RTGS" for the improvement of the efficiency and minimizing errors in payment processing through PRISM system, SBP decided under Section 3 of Payment Systems and Electronic Fund Transfer (PS&EFT) Act 2007 that the participants' banks shall implement Straight Through Processing (STP) for automated processing of transactions through PRISM system.

The Bank of Khyber has setup the STP with PRISM-RTGS and in compliance of point #: 3(iv) of the said circular, services of third party audit & security assessment firm for the given below scope of work is required before going live. Detailed Scope of work is attached at Annexure – B of the document.

Bidders are required to submit their sealed proposals (EOI) in line with Khyber Pakhtunkhwa Procurement Rules 2014 to the office of the **Head Procurement Division, The Bank of Khyber** on or before 09-05-2019. And shall be opened on same day at 4:00 PM at The Bank of Khyber, Head Office.

Proposals should be in the prescribed format along-with all the relevant documents as per the **Terms & Conditions** and **Bidder Eligibility Criteria**.

Terms and Conditions

- a) Bidder is required to submit its Company Profile along-with Proposal that must comply with the following **Bidder Eligibility Criteria** (Annexure – A).
- b) Proposals submitted Late / after due date and time or Incomplete will not be considered.
- c) Only Shortlisted Firms will be invited to submit their Technical and Financial proposals.
- d) The competent authority reserves the right to accept or reject any proposal as per KPPRA rules.
- e) All sections in the bid should be adequately flagged and numbered.
- f) Bidder is required to assign a dedicated onsite Project Manager to manage the project and report to the stakeholders as per requirement.
- g) In case of consortium, the bidder must submit:
 - The details of the consortium with roles and responsibilities of each partner.
 - The original stamped consortium agreement shall be attached along-with the Bid Document.
 - The same should be endorsed by an authorized representative of the prime bidder. The Prime bidder will be the single point of contact with the Bank for the project undertaking.
 - No change in the constitution of the consortium (prime bidder/members of consortium/stakes of any member etc.) will be allowed without explicit approval of the Client.
- h) Bids not complying with all the given clauses in this tender document are liable to be rejected.

Annexure – A

Bidder Eligibility Criteria

Bidder is required to submit its Proposal in accordance with the **Mandatory** requirements mentioned in the Bidder Eligibility Criteria. Failing to which the proposal will not be considered.

#	Mandatory Requirements	Attached (Yes / No) Reference (Page / Annexure)
1	Name of the Bidding Firm. Name of authorized contact person along-with his designation, contact number, email address and postal address.	
2	Proposed Methodology and Processes Describe the proposed methodology and processes to audit and conduct security assessment of STP with PRISM RTGS in accordance with SBP's PSD Circular No. 2 of 2016.	
3	The firm should be SBP's Category 'A' Auditing Firm.	
4	The bidder should provide its FBR registration certificate (NTN) along-with Registration of Incorporation under the laws of Pakistan.	
5	The bidder should provide Undertaking on stamp paper that it is not being blacklisted by any of the Provincial / Federal Government or organizations of the State / Federal Government in Pakistan. And must provide List of arbitration/legal suits/unsettled disputes with the financial sector clients (if any) in last five years.	
6	The bidder must submit Annual Audited Report for the last 03 Financial years. Annual Audit Report including Balance Sheet, Income Statement and Profit & Loss accounts along with auditors' notes for the last three audited years should be submitted.	
7	The bidder must have legal presence in Pakistan. The firm must submit List of Offices across Pakistan.	
8	The bidder/prime bidder (in case of consortium) should have experience in conducting Information Systems (IS) Audit and Security Assessments such as vulnerabilities assessments and penetration testing. The bidder shall provide a list of completed projects similar in nature along-with references and contact numbers for any Financial Institution / Banking Sector.	
9	Bidder is required to submit the detailed profile of Project Manager who will be nominated / assigned for the management of the project.	
10	The bidder should have enough Technical Strength at its end to complete the project within stipulated time. List of Project team of the Company along-with their Profiles to be submitted.	
11	Firm should be an active tax payer under the laws of Pakistan and must provide Sales Tax certificate, GST, etc. along-with KPRA (Khyber Pakhtunkhwa Revenue Authority) Registration certificate.	

Technical Requirements / Scope of Work

The scope and deliverables of the assignment as required by The Bank of Khyber in accordance with SBP's PSD Circular No.2 of 2016 dated: Jan 19, 2016 clause #: 3(iv) regarding third party audit and security assessment on STP with PRISM-RTGS are mentioned below:

The activities should include but not limited to the following:

- Business Requirements should be validated to ensure completeness
- Compliance review to check the design and configuration of complete infrastructure (systems level, network level etc.) architecture in light of SBP guidelines
- Review and testing in-respect of correctness and completeness of functional controls for the fulfillment of business requirements
- Review of security controls at database level
- Review of security controls at application & operating system levels
- Review of security controls at related network level
- Review of physical controls for the protection of related infrastructure
- Review of related procedures & processes
- Review of controls to protect the data in transit & rest
- Review of controls to ensure the confidentiality of customer data
- Review arrangement for Business Continuity Planning (BCP) and Disaster Recovery Planning
- Review of entire systems, infrastructure, processes & procedures etc. in adherence to all relevant laws, rules, regulations and instructions issued from time to time by relevant authority / regulatory body
- Recommend appropriate controls (administrative including processes & procedures etc., physical and logical levels) to plug-in the identified gaps. The recommendation should be detailed, easy to understand and follow.
- Firm should revalidate and certify the implementation of requisite controls, testing results and process design.
- Firm should ensure the compliance of the clause 3(iv) of SBP's PSD Circular No. 2 of 2016 dated Jan 19, 2016

Required Deliverables

Bidders are required to provide the following:

- Comprehensive Audit and Security assessment report that should include assessment methodology, risks severity ratings, impact, vulnerability references (OWASP, CIS, CVE, CWE, OSVDB etc.), detailed recommendations, etc. related to this project.
- Further, the bidder shall provide editable copy of report for BOK's internal purposes without any additional fee.

***Head Procurement, Head office,
The Bank of Khyber, 29 A, The Mall, Peshawar Cantt.
Phone: 091-5261117, 091-5275352***