THE BANK OF KHYBER

Expression of Interest (EOI)

Acquisition of 3rd Party Services for Bank's Payment systems and Infrastructure's Vulnerability Assessment, Penetration Testing and Compromise Assessment as per SBP Requirement

---

Last Date for Submission: **07-10-2019 at 11:30AM**

Opening Date: **07-10-2019 at 12:00AM**

Tender No. BOK/PROC/IT/02/Sep/2019

Description of Work

A. Introduction

State Bank of Pakistan in its PSD Circular No.9 of 2018 regarding "Security of Digital Payments" has mandated Banks to conduct Independent 3rd Party review/assessment of their alternate delivery channels (ADCs) and payment systems including but not limited to card systems, RTGS, SWIFT, Internet/Mobile banking and agent-based/Branchless Banking etc. In this respect, 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 **Incharge Procurement Department, The Bank of Khyber** on or before **07-10-2019 at 11:30AM**. And shall be opened on same day at **12:00AM** 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**.

Note: The prospective bidder is expected to examine the EOI Document carefully, including all Terms & Conditions and Annexures. Failure to furnish all information required by the EOI documents or submission of a Bid not substantially responsive to the EOI Documents in every respect would result in the rejection of the Bid.

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
1	Name of the Bidding Firm. Name of authorized contact person along-with his designation, contact number, email address and postal address.	
2	Bidders having minimum 5 (Five) years of relevant experience of vulnerability assessment and penetration from the date of incorporation of the company / registration of the firm shall be eligible to participate.	
3	**Proposed Methodology and Processes** Describe the proposed methodology for conducting of vulnerability assessment, penetration testing and compromise assessment of bank's payment systems and infrastructure as per SBP requirement given in its PSD Circular No. 9 of 2018 dated Nov. 28, 2018.	
4	Bidder should submit detailed profile including copies of industry professional level certificates of its certified assessors / testers.	
5	The Bidder should be active Tax/Sale Tax/GST payer, copy of latest returns to be attached	
6	Copy of Registration of Incorporation under the laws of Pakistan with SECP to be attached.	
7	The bidder should provide Undertaking on stamp paper duly attested by Notary Public 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.	
8	The bidder must submit **Annual Audited Report** for the last 03 Financial years.	
9	The bidder must have legal presence in Pakistan. The firm must submit **List of Offices** across Pakistan.	
10	The bidder or prime bidder (in case of consortium) shall provide a list of	

	completed projects along-with references for any Financial Institution / Banking Sector: ▪ in conducting similar assignments (i.e. for the compliance of above-mentioned SBP requirement) and ▪ Providing services for penetration testing, vulnerability assessment and compromise assessment to any Financial Institution / Banking Sector. ▪ Bidder should have completed at least two consulting projects with similar scope for Commercial banks in Pakistan. As a proof, work order or work completion certificate(s) shall be submitted by the bidder. Only those firms are considered who have successfully performed all the following assignments in the banking industry by themselves for the compliance of SBP's requirement as mandated in its circular no. PSD Circular No. 09 of 2018. ▪ Compromise Assessment ▪ Vulnerability Assessment ▪ Penetration Testing ▪ Foot printing ▪ Scanning ▪ Enumeration ▪ Password Attacks ▪ Network Hacking ▪ Exploitation ▪ Backdoors and Rootkits ▪ Website Hacking These firms must submit clear evidences for the same.	
11	The bidder must use those soft wares/tools having legal ownership for vulnerability assessment and penetration testing through professionals having relevant information security certifications and experience.	
12	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.	
13	Copy of active registration certification with KPRA (Khyber Pakhtunkhwa Revenue Authority).	
14	Bidder is required to assign a dedicated onsite Project Manager to manage the project and report to the stakeholders as per	

	requirement. Copy of CV and certifications of the Project Manager to be attached	
15	Bidders must sign and stamp each paper of this EOI document, and submit with proposal.	

Annexure – B

Objective

The main objectives of this exercise are the following:

1. To ensure compliance with SBP requirement as laid out in PSD Circular No. 9 of 2018 regarding "Security of Digital Payments" Clause No. 2.
2. To have assurance that BOK's IT Infrastructure is secured against internal and external threats or intrusions.
3. To have assurance that BOK's Payment systems are not compromised and jeopardizing the confidentiality, integrity and availability of the data, systems and related infrastructure.
4. To test and verify the security of the Information Technology systems and network for ensuring the effectiveness of deployed security measures.
5. Verify the perimeter security controls and identify any areas of improvement.
6. Verify the security controls associated with internal and external web applications that are used by BOK.
7. Identify and recommend suitable safeguards with the aim to strengthen the level of protection of the BOK's IT infrastructure.

Scope of Work:

Services of third-party service provider are required to conduct vulnerability assessment and penetration testing for the compliance of SBP's requirement laid down in the PSD Circular 9 of 2018 related to "Security of Digital Payment".

Additionally, service provider is also required to identify any already compromised payment card systems; related platforms, applications, network infrastructure etc. through compromise assessment.

Detailed scope of work includes the following requirements (not limited to):

The service provider is required to perform the following tasks:

- Study BOK's environment to identify related systems, databases, web applications, network components in-respect of payment systems and critical infrastructure.

Vulnerability Assessment & Penetration Testing:

- The assessment and testing will be conducted prominently on the following systems and related infrastructure, but not limited to:
  - Messaging Systems
  - Web Applications
  - Databases
  - Network components

- Payment Card Environment
- SWIFT
- RTGS
- REMITIX
- All ADC Channels working via IRIS
- Etc.

- Perform vulnerability assessment of BOK's critical IT Infrastructure including applications, databases, network components, etc. to identify potential and inherent weaknesses in the administrative, physical and technical controls that can lead to compromises.
- Recommend appropriate administrative, physical and technical countermeasures to plug in the identified vulnerabilities. Recommendation should be easy to understand and follow.
- Perform external and internal penetration testing of the payment systems to verify the resilience level against a launched attack.
- The penetration testing should be performed to simulate various types of attacks that can compromise the confidentiality, integrity and availability of the payments systems.

Recommend appropriate administrative, physical and technical measures and controls to elevate the resilience level against different types of attacks that has proven to be successful during penetration testing.

Compromise Assessment:

- The compromise assessment conducted prominently on the following systems and related infrastructure:
  - Payment Card Environment
  - SWIFT
  - RTGS
  - REMITIX
- Perform assessment to detect potential targets for threats actors through analysis of related data.
- Perform compromise assessment on payment systems to identify any already compromised systems, applications, network components etc. through Indicator of Compromise (IoC) and Indicator of Attack (IoA). These should be properly documented and be part of main report.
- Discovery of APT's through deployment of breach detection systems during the assessment.
- Through engaging BOK team perform remediation steps and measures to confine the effect and stop the active attack (if any).
- Recommend effective countermeasures to provide resilience against the identified attacks.

Required Documentation:

- Separate document detailing the payment systems, their related applications, network components etc. including related diagrams.
- Separate report of penetration testing and vulnerability assessment of payment systems with easy to understand recommendations and steps to plug in the identified vulnerabilities and elevate the resilience level.
- Separate report of penetration testing and vulnerability assessment of systems, applications, network services, etc. other than payment systems with easy to understand recommendations and steps to plug in the identified vulnerabilities and elevate the resilience level.
- Separate report regarding penetration testing and vulnerability assessment of SWIFT Infrastructure.
- Network Diagram & Configuration Assessment Report of SWIFT Infrastructure as per SWIFT Customer Security Program
- Network Diagram & Configuration Assessment Report of Payment Card Environment as per PCI-DSS, CIS or any other well-known benchmark etc.
- Network Diagram & Configuration Assessment Report of REMITIX
- Separate report of compromise assessment on potential and inherent weaknesses in the administrative, physical and technical controls of the payment systems that can lead to compromises or if comprised already. The report should include at least the following but not limited to:
  - Results of the Compromise Assessment in detail and how these are obtained
  - List of compromised assets (i.e. application, operating systems, databases, network components, etc.)
  - Type of compromise
  - Reasons to reach the conclusion
  - Controls circumvented
  - Remedial actions taken to clean and stop the future similar compromise i.e. proactive and reactive measures for incident response
  - Recommendations for preventative, detective and response/readiness measures.

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.
h) 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.
i) Bids not complying with all the given clauses in this tender document are liable to be rejected.
j) The Bank of Khyber will not be responsible for any costs or expenses incurred by bidders in connection with the preparation or delivery of bids.
k) Bidders are essentially required to provide correct and latest postal/email addresses, phone/mobile/fax numbers for actively and timely communication.
l) For any query, clarification regarding EOI documents contents, the applicants may send a written request at least 5 days prior to the opening date through registered posts/Courier Service.

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