



BOK Penetration Testing



Request for Proposal (RFP)

BOK PENETRATION TESTING

Date of Issue	
Closing Date	
Place	
Enquiries	

IT Division, Head Office, The Bank of Khyber, 4th Floor, State Life Building, Peshawar
Phone: 091-5279690, 091-5274399. UAN: 091-111-95-95-95. Fax: 091-5286769.



BOK Penetration Testing

Table of Contents

1. Project Introduction	3
1.1 About The Bank of Khyber	3
1.2 Critical Success Factors	3
1.3 Contact Details	4
2. Project Details	5
2.1 Scope of work.....	5
2.2 Project Activities	5
2.3 Deliverables.....	5
3. RFP Information	6
3.1 Minimum Requirements for RFP Response	6
3.2 Vendor Evaluation Criteria	6
4. General Instructions	8
4.1 RFP Terms & Conditions.....	8
4.2 Confidentiality.....	8



BOK Penetration Testing

1. Project Introduction

This Request for Proposal (RFP) is being issued for the, **Penetration Testing of Information Technology Infrastructure**, as part of regular process of verifying the implemented security controls and thus to further enhance the security of the IT systems and achieve improved and secure IT infrastructure.

Bank of Khyber invites **technical and financial proposal** from the selected vendors for the execution of the Penetration Testing of IT infrastructure. The proposal should include the timelines and execution schedule.

Financial proposal should provide cost of external tests, internal tests, websites tests separately. It should mention vendor's terms of payment, availability status and expected delivery period. Financial proposal should be in local currency (PKR), inclusive of all applicable duties, taxes and charges.

The vendor must submit a proposal substantially aligned to the requirements included in the RFP. Bank of Khyber's evaluation of the proposal for awarding the project shall be based on the original proposal. However, BOK may decide to incorporate or truncate items on the basis of alternate proposal submitted by the successful bidder, if the proposal has been evaluated technically compliant with best combination of price and other criteria.

Bank of Khyber reserves the right at the time of award to minimize the scope in the RFP. In addition, Bank of Khyber may delete any item from the RFP and the bid price shall be reduced accordingly.

1.1. About The Bank of Khyber

The Bank of Khyber was established in 1991 through Act No. XIV, passed by the Provincial Legislative Assembly of the KHYBER PAKHTUNKHWA Province of Pakistan. It was awarded status of a scheduled bank in September 1994. The Bank of Khyber enjoys a unique position, and stands out amidst the other

IT Division, Head Office, **The Bank of Khyber**, 4th Floor, State Life Building, Peshawar
Phone: 091-5279690, 091-5274399. **UAN:** 091-111-95-95-95. **Fax:** 091-5286769.



BOK Penetration Testing

banks operating within Pakistan, and has the privilege of being bracketed amongst the only three government banks in the country.

BOK has a total of **130 branches** all over the country and BOK's client base is located in major cities of Khyber Pakhtunkhwa, Punjab, Sindh, Baluchistan and Azad Kashmir.

With high reliance on technology for managing and growing business, BOK considers information security as a major business enabler. In continuation to the enhancement of IT security of its architecture, BOK wants to take effective implementation of controls by acquiring services of professional Penetration Testing organizations.

1.2. Critical Success Factors

The successful Penetration Testing of BOK's IT infrastructure will result in:

- Identification of vulnerabilities, Security Risks, Threats & gaps to which BOK's IT infrastructure, application and data is exposed;
- Recommendations to remediate the identified security risks, threats and vulnerabilities;
- Timely completion of the assessment & submission of the final report

1.3. Contact Details

Primary Contact Details:

Secondary Contact Details:

Financial contact:



BOK Penetration Testing

2. Project Details

2.1. Scope of Work

The proposal should reflect each of the sections listed below, highlighting attack motivations pertaining to BOK's environment:

- Network Architecture Designs Reviews.
- Wireless Network Assessment and Penetration Testing
- Server Configuration Reviews.
- VPN Configuration Reviews.
- Website Penetration Testing

Objectives:-

The goal of this exercise is to ensure that reasonable protection is in place for general and particular threats that may exist for BOK's IT systems and infrastructure including but not limited to the following:

1. To test and verify the security of the Information Technology systems and network so as to ensure the effectiveness of deployed security measures.
2. Verify the perimeter security controls.
3. Verify the security setup and configuration of internal/External BOK's IT infrastructure. It will include the associated networks and systems with a perspective of ensuring CIA and authenticity of data and information systems.
4. Verify the security associated with web applications / website that are used by Bank of Khyber.
5. Identify and recommend safeguards, suited to BOK's environment, with the aim to strengthen the level of protection of the BOK's IT infrastructure.

Bank of Khyber desires to engage the services a well reputed IT security company to conduct the following services i.e, Server Configuration Reviews, Network Security Posture Assessment:

- **Internal & External Penetration Testing**
 - ✓ Password Cracking
 - ✓ Router Testing
 - ✓ Denial of Service (DOS) Testing
 - ✓ Distributed DOS testing
 - ✓ Containment Measures Testing
 - ✓ Ensuring optimum performance of the System.
- **Network Architecture Designs/ Reviews**
 - ✓ Network Scanning
 - ✓ Review of Network Monitoring Software (NMS).

IT Division, Head Office, The Bank of Khyber, 4th Floor, State Life Building, Peshawar
Phone: 091-5279690, 091-5274399. UAN: 091-111-95-95-95. Fax: 091-5286769.



BOK Penetration Testing

- ✓ **Network Infrastructure Review**
- ✓ **Security of Data Transmission**
- **Web Application Assessments**
- **Firewall Diagnostics Review**
- **IDS/IPS Diagnostic Review**
- **Security Awareness Training**

2.2. Project Activities

Participating vendors are required to submit their proposals specifically covering the following activities and functions to be assessed

Sr. No.	Activities	Functions and Scope
1	Project Orientation	Exchange of required information with respect to all critical systems.
2	Security Assessment	Security risk assessment of all critical systems.
3	Final Report and Recommendations	Report including level of risk, and recommendations.

2.3. Deliverables

The selected vendor will submit report to the BOK and recommended mitigating action plan to address the identified issues. Include descriptions of the types of reports used to summarize and provide detailed information on Information security risks, vulnerabilities, and the necessary countermeasures and recommended corrective actions.



BOK Penetration Testing

3. RFP Information

3.1. Minimum Requirements for RFP Response

The following information must be provided in each vendor's proposal in soft form (CD) and hard copy via courier service:

1. Project plan
 - Process for each activity and functionality
 - Duration of each activity
 - Expected involvement of BOK's staff for each activity
 - Facilities required from the BOK
2. Vendor's profile and experience
 - One page summary of company profile (business, coverage, staff, etc.)
 - Details of successful Penetration Testing in Pakistan
 - Number of skilled resources in Pakistan (Information Security)
3. Detailed profiles of the project team
4. List and profile of affiliated partners/practitioners (if applicable)
5. Cost (sub divided per activity in the project details section)
6. Contact information of project team leader and team members

3.2. Vendor Evaluation Criteria

Any award to be made pursuant to this RFP will be based upon the proposal with appropriate consideration given to operational, technical, cost, and management requirements. Evaluation of offers will be based upon the Vendor's responsiveness to the RFP and the total price quoted for all items covered by the RFP.

The following elements will be the primary considerations in evaluating all submitted proposals and in the selection of a Vendor or Vendors:

1. Completion of all required responses in the correct format.
2. The extent to which Vendor's proposed solution fulfills BOK's stated requirements as set out in this RFP.
3. An assessment of the Vendor's ability to deliver the indicated service in accordance with the specifications set out in this RFP.
4. The Vendor's stability, experiences, and record of past performance in delivering such services to at least five different financial institutions/organizations.
5. Provide the number of years that a firm has been in business and the firm's qualifications and experience performing similar Penetration Testing.
6. Provide a list of similar assessments that the firm has performed within the last two years.

IT Division, Head Office, The Bank of Khyber, 4th Floor, State Life Building, Peshawar
Phone: 091-5279690, 091-5274399. UAN: 091-111-95-95-95. Fax: 091-5286769.



BOK Penetration Testing

7. Provide a list of name(s) and professional qualifications, responsibilities and resumes of the managerial, technical and support staff identified to conduct security test.
8. Description of methodology that will be used to perform the assessment, approach that will be taken to gain an understanding of the IT function and the criteria that will be used to identify security risks, vulnerabilities as well as evaluation controls.
9. Statement of compliance with the guidance of one or more of the professional organizations that have promulgated industry standards and guidelines for conduction penetration testing.
10. Availability of sufficient high quality Vendor personnel with certifications such as Certified Information System Security Professional (CISSP), Certified Ethical Hacker (C|EH), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), GIAC Certified Penetration Tester (GPEN), ISO 27001 Lead Auditor, Certified in Risk and Information System Control (CRISC) and proven references of conducting the similar activities preferably in a bank.
11. Availability / appointment of a Project Manager having minimum 5 years of experience in Managing IT across banking sector.
12. Overall cost of Vendor's proposal.
13. Documents should include client list with the affidavit as not black listed or involved in litigation.



BOK Penetration Testing

4. General Instructions

Respondents of this RFP are required to study its contents carefully, including the following:

4.1. RFP Terms and Conditions

1. The Bank of Khyber invites proposal from reputable Companies/TRI Partner for the supply, delivery and Service Providers.
2. All bids must be accompanied by a call deposit of two percent (2%) of total bid amount in favor of the Bank and must be delivered to the HEAD IT DIVISION, THE BANK of KHYBER.
3. Call deposit must be attached with financial proposal in sealed envelopes.
4. **All Bids must be submitted and will be opened on same day dated 31-08-2016 Wednesday at 10:00AM and the opening timings will be 11:00AM at BOK I.T Division.**
5. **If any bids submitted late on the date of opening after opening times will not be entertained.**
6. The Tender Bids must be in sealed envelopes. Proponents applying for bids should submit two separate sealed bids/envelopes, one for Technical Proposal and one for Financial Proposal.
7. The Technical Proposal should contain all the bid items (Specification of bid) without quoting the price and must list the support plan (After Sale Service Plan) during warranty period.
8. **If the Technical Specification does not meet BOK requirement, then financial proposal shall not be opened.**
9. 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.
10. Services must be provided within **(4 – 6)** weeks of issuance of purchase order.
11. All prices quoted must include all Taxes applicable, such as GST, Income Tax (Included all Taxes).
12. **In case of failure to provide the services. The work order should be awarded to second lowest.**
13. Failure to provide the services within **(4 - 6)** weeks' time period will invoke. In addition to that, Call Deposit (CDR) amount will be forfeited.
14. Company seal/stamp must be fixed on Technical specification and financial proposal.
15. Bidders must submit at least one bid that matches or is better than the advertised specifications and are free to quote more options each clearly marked as option 1, option 2 in separate envelopes.
16. **No negotiations and revised bids will be allowed.**

The Penetration Testing and I.T Risk Assessment/Re-Assessment services should be provided by the contractor to The Bank of Khyber.



BOK Penetration Testing

4.1. Confidentiality

This RFP and BOK's process of evaluating sourcing opportunities, as well as the timing and content of any meeting, discussions and negotiations between BOK and the Respondent, will be deemed "Confidential Information" for the purposes of the Non-Disclosure Agreement (NDA).

Respondents must recognize and acknowledge that BOK operates in a highly competitive business environment and, for that reason, expects that Respondents will treat all materials and data provided by BOK as confidential.