Penetration Testing

Request for Proposal
1. RFP INFORMATION

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 technical and financial proposal must be submitted in two separate sealed envelopes latest by 12th April 2013 marked to Incharge Procurement, I.T Division, the Bank of Khyber at 4th Floor, Statelife Building, the Mall, Peshawar Cantt. Peshawar.

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.

Provision for any price escalation adjustment included in the proposal shall not be taken into consideration.

Bank of Khyber reserves the right to accept or reject any proposal and to withdraw the process and reject all proposals, at any time prior to award of Contract, without thereby incurring any liability to the affected bidder(s) of any obligation to inform the affected bidder(s) on the grounds for BOK’s action.

Bank of Khyber reserves the right at the time of award to increase or decrease 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.
2. **INTRODUCTION**

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 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 **80 branches** all over the country and BOK’s client base is located in major cities of Khyber Pukhtunkhwa, 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.
3. 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 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.
4. PROPOSAL REQUIREMENT

Vendor’s proposal in response to this RFP will be incorporated into the final agreement between BOK and the selected vendor. The submitted proposals are suggested to include each of the following sections:

1. Executive Summary
2. Approach and Methodology
3. Project Deliverables
4. Project Management Approach
5. Detailed and Itemized Pricing
6. Appendix: References
7. Appendix: Company Overview

4.1 EXECUTIVE SUMMARY

This section will present a high-level synopsis of the vendor’s responses to the RFP. The Executive Summary should be a brief overview of the engagement, and should identify the main features and benefits of the proposed work.

4.2 SCOPE, APPROACH AND METHODOLOGY

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.
- PCI Quarterly Scan.
- PCI Report on Compliance Assessment or Gap Analysis.
- Virtual Infrastructure Security Assessment.
- Website Penetration Testing

4.3 DELIVERABLES

Include descriptions of the types of reports used to summarize and provide detailed information on security risk, vulnerabilities, and the necessary countermeasures and recommended corrective actions.

4.4 PROJECT MANAGEMENT APPROACH

Include the method and approach used to manage the overall project and client correspondence. Briefly describe how the engagement proceeds from beginning to end.

4.5 DETAILED AND ITEMIZED PRICING

Include a fee breakdown by project phase and estimates of travel expenses if required. Separate quotations should be provided for each testing type stated in 4.2.

4.6 APPENDIX: REFERENCES

Provide reference(s) for which the vendor has performed similar work.

4.7 APPENDIX: COMPANY OVERVIEW

Provide the complete name, address, phone numbers, fax, emails and contact person related details etc.
5. EVALUATION FACTORS FOR AWARD

5.1 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.
5. 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.
6. Availability / appointment of a Project Manager having than 10 years of experience in Managing IT across banking sector.
7. Overall cost of Vendor’s proposal.
8. Documents should include client list with the affidavit as not black listed or involved in litigation.

BOK may, at their discretion and without explanation to the prospective Vendors, at any time choose to discontinue this RFP without obligation to such prospective Vendors.
6. **SCOPE OF WORK**

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).
  - Network Infrastructure Review
  - Security of Data Transmission

- **Web Application Assessments**

- **Firewall Diagnostics Review**

- **IDS/IPS Diagnostic Review**

- **Security Awareness Training**

### 6.1 DELIVERABLES

At the conclusion of the assessment, BOK requires written documentation of the approach, findings, and recommendations associated with this exercise. The documentation should consist of the following:

- Detailed technical report
- Executive summary report

#### 6.1.1 DETAILED TECHNICAL REPORT

A document developed for the use of BOK’s technical staff which discusses: the methodology employed, positive security aspects identified and their importance, detailed technical vulnerability / threat findings, an assignment of a risk rating for each vulnerability / threat, supporting detailed exhibits for vulnerabilities when appropriate, and detailed technical remediation steps.

#### 6.1.2 EXECUTIVE SUMMARY REPORT

A document developed to summarize the scope, approach, findings and recommendations, in a manner suitable for senior management.
7. CONTACT INFORMATION

7.1  TECHNICAL CONTACT

Any questions concerning technical specifications or Statement of Work (SOW) requirements must be directed to:

<table>
<thead>
<tr>
<th>Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Phone</td>
<td></td>
</tr>
<tr>
<td>FAX</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td></td>
</tr>
</tbody>
</table>

7.2  CONTRACTUAL CONTACT

Any questions regarding contractual terms and conditions or proposal format must be directed to:

<table>
<thead>
<tr>
<th>Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Phone</td>
<td></td>
</tr>
<tr>
<td>FAX</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td></td>
</tr>
</tbody>
</table>
8. PENETRATION SUCCESS CRITERIA

Achievement of anyone of the following scenario would qualify as successful penetration:

- Access to internal resources (like file server, DNS or mail server, Web application server etc).
- Reading restricted files (reading / browsing restricted folders, Web application files, OS critical files etc).
- Altering restricted files (planting Trojan / rootkit, modifying files at file server or modifying OS files etc).
- Reading transaction data.
- Executing a program or transaction (executing restricted files like .exe, .batch or installing programs, injecting false transactions etc).
- Access to any user account.
- Access to administrative accounts.
- Controlling network management systems.
- Demonstrating ability to control resources (like desktops, servers, devices etc).
- Website defacement.
- Denial of service, as a result of modifications in internal systems.