Request for Proposal (RFP)

BOK INFORMATION TECHNOLOGY RISK ASSESSMENT

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.

Table of Contents

1. Project Introduction

The Bank of Khyber is seeking the services of a qualified entity that is experienced in assessing Information Technology (IT) risks for the purpose of performing a risk assessment of the BOK's IT environment and providing input to the IT Risk Plan. IT is a key component in the process to continuously improve the BOK's operations by improving services and reducing costs. Due to the diversified operations within the BOK, several types of applications and platforms exist. Risks associated with IT, such as data integrity and reliability, availability, security and efficiency, need to be effectively managed.

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 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 IT Risk Assessment organizations.

1.2. Critical Success Factors

The successful IT risk assessment of BOK's IT infrastructure will result in:

- Identification of risks & gaps to which BOK's IT infrastructure, application and data is exposed;
- Identification of gaps in the implementation of BOK's information security policy;
- Recommendations to remediate the identified risks/gaps;
- Timely completion of the assessment & submission of the final report

1.3. Contact Details

Primary Contact Details:

Secondary Contact Details:

Financial contact:

2. Project Details

2.1. Scope of Work

Objectives:-

1. Determine adequacy of risk control in BOK;
2. Analyze and evaluate the quality of processes, routines and controls of the following general IT processes:

✓ Organization and management of IT operations;
✓ LAN/WAN network infrastructure;
✓ Application development and maintenance;
✓ Computer operations and disaster recovery; and
✓ IT application, network(LAN/WAN) and infrastructure security

3. Identify and describe IT lapses/loopholes along with mitigating controls
4. Identify and describe high-risk areas;
5. Identify and describe mitigating controls for the defined high-risk areas and compare the existing control structure with the IT industry's best practices;
6. Identify opportunities for improvement and develop practical recommendations for each opportunity identified;
7. Test adequacy of BOK business continuity plans and procedures; and
8. Assess adequacy of governance procedures and structures in managing risks and compliance to relevant regulations.

Implementation:-

1. Assess the effective information technology infrastructure (hardware, networks, software, people and processes) to effectively support the current and future needs of the business in an efficient, cost-effective and well controlled fashion;
2. Assess the robustness of the local area network infrastructure;
3. Assess the processes governing the application development and maintenance area;
4. Assess business continuity plans and procedures;
5. Assess general IT application, network and infrastructure security;
6. Risks associated with inappropriate access to systems, data or information. It includes the risks of improper segregation of duties, risks associated with the integrity of data and databases, and risks associated with information confidentiality; and
7. Assess physical access control procedures to BOK IT data center.
8. Risk assessment and Re-assessment – identification of strengths and opportunities for improvements (risk areas and mitigating controls).
9. Preparation of Cyber security action plan along with implementation.
10. Development of Cyber Security Policy.
11. Development of Information Risk Register.

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 corrective action plan to address the identified issues. Include descriptions of the types of reports used to summarize and provide detailed information on Information and Information Resources Inventory, IT Risk Assessment Report, IT Controls Assessment Report as well as Cyber Security Policy along with course of action and the necessary countermeasures with recommended corrective actions.

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 I.T risk assessments 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 IT risk assessments.
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.

7. Provide a list of name(s) and professional qualifications, responsibilities and resumes of the managerial, technical and support staff identified to conduct the assessment.
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 risk and 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 conducting IT risk Assessments.
10. Recommendations and descriptions of continuing IT audit plan.
11. Availability / appointment of a Project Manager having more than 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.

4. General Instructions

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.

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 bids 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 envelops.
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.

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.