REQUEST

FOR

PROPOSAL

For Full Scope Information Technology Audit

1. Executive Summary

We are pleased to present this proposal for the outsourcing of the IT audit services for Afghan United Bank. We at AUB are dedicated to maintain the highest standards of IT security, IT compliance, and IT operational excellence, we recognize the critical importance of a robust and comprehensive IT audit.

In an increasingly interconnected and digital landscape, the security and integrity of our information technology systems are paramount. We are seeking a qualified and experienced partner to collaborate with us in conducting a thorough assessment of our IT infrastructure, security protocols, and compliance measures. By outsourcing the IT audit to a specialized firm, we aim to leverage expert insights and best practices to enhance our cybersecurity posture and ensure the safeguarding of sensitive financial data.

This proposal outlines our vision, objectives, and expectations for the IT audit outsourcing initiative. We invite prospective vendors with proven track records in conducting IT audits for financial institutions to review this document and provide a comprehensive response that aligns with our goals.

2. Corporate Background

Afghan United Bank is a full-fledged privately-owned commercial bank incorporated on October 4, 2007. The Bank obtained its banking license under the Banking Laws of Afghanistan from the Central Bank of Afghanistan (DA Afghanistan Bank).). The Bank is currently operating through 33 branches in Kabul, Nangarhar, Kandahar, Balkh, Herat, Kunduz, Parwan, Helmand, Nimroz, Khost , Farah, Baghlan, Faryab, Kapisa, Zabul, Bamyan and other big cities of the country. The bank is offering financial products and services in both Conventional and Islamic Banking across these branches.

3. Objective of the Assignment

The primary objective of this assignment is to conduct a comprehensive IT audit of Afghan United Bank's information technology systems, databases and applications, security measures, compliance practices and governing policies.

The engagement aims to achieve the following key goals:

1. Assessment of IT Infrastructure: Thoroughly evaluate the bank's network architecture, databases, core banking applications, depending hardware and software, and communication protocols to identify strengths, weaknesses, and areas for improvement.

2. Assessment of the IT Governance: Evaluate the best practices implemented, policies in practice including the assessment of the SLAs in place, human resources alignment and the values delivered.

3. Enhanced Data Security: Assess the effectiveness of the bank's data security protocols, access controls, and data handling practices. Identify vulnerabilities and recommend measures to strengthen data protection.

4. Regulatory Compliance: Review the bank's adherence to industry regulations, standards, and mandates of DAB and other relevant requirements. Highlight areas of non-compliance and provide actionable recommendations.

5. Risk Identification: Identify potential risks, threats, and vulnerabilities that could impact the bank's IT systems, data integrity, and customer trust. Prioritize risks based on their potential impact and likelihood.

6. Business Continuity and Disaster Recovery: Evaluate the bank's disaster recovery and business continuity plans, ensuring they are robust and effective in maintaining operations during unforeseen disruptions.

7. Actionable Recommendations: Provide clear and actionable recommendations to address identified vulnerabilities, strengthen security measures, and enhance compliance efforts. Recommendations should be tailored to AUB's unique environment.

8. Knowledge Transfer: Share insights, best practices, and industry trends with AUB's audit, IT, CBS and E-Banking teams to foster ongoing improvement in IT infrastructure and security practices.

4. Government withholding tax

Pursuant to Article 72 in the Afghanistan Tax Law effective March 21, 2009, Afghan United Bank is required to withhold "contractor" taxes from the gross amounts payable to all Afghan for-profit subcontractors/vendors. In accordance with this requirement, Afghan United Bank shall withhold two percent (2%) tax from all gross invoices to Afghan contracts under this Agreement with active business license from Ministry of Commerce & industry Afghanistan whereas the foreign partners'/vendors companies bidding for this RFP shall include 7% tax and the mentioned percentage will be deductible upon invoice payment.

5. Government license & Bank Accounts

The participating company shall provide a copy of the organization's Business license and TIN (Tax Identification Number). Foreign companies shall also submit the country issued license. Further companies are required to have Bank accounts with official license and shall provide the Bank statement as of date signed and stamped by the Bank.

6. Proposal Currency

The proposal currency should be Afghani for local participating companies and AED/EUR/INR for foreign participating company would be preferred.

7. Acceptance/Rejection

Afghan United Bank reserves the right to accept or reject any or all bids and to annul the bidding process at any time/stage, without thereby incurring any liability to the affected bidder(s) or any obligations to inform the affected bidder(s) of the grounds for AUB action.

8. Scope of Work

The scope of this engagement encompasses a comprehensive IT audit that will thoroughly assess and evaluate the information technology systems, databases, core banking applications, depending Hardware and Software, security protocols, and compliance measures at AUB.

A description of the scope is enumerated in brief as under and in detail. However, the Bank reserves its right to change the scope of the RFP considering the size and variety of the requirements and the changing business conditions. The selected vendor will be responsible for the following key areas:

i. Audit of Information Technology Policies, Environment and SLAs

Evaluate the bank's Information Technology policies, technology environment, and adherence to Service Level Agreements (SLAs) within the IT. This aspect of the audit will provide insights into the bank's IT governance, infrastructure, and performance metrics. This will include the review of:

1. Information Technology Policies
2. CBS Policies
3. EBD Policies
4. Roles and Responsibilities
5. Software Checklists
6. PR Environment
7. DR Environment
8. Physical Security
9. Change & Incident Management
10. Business continuity and Disaster recovery plan
11. Vendor SLAs and Management

ii. Network Infrastructure Assessment & Security audit

Conduct a detailed review of the bank's network architecture, including hardware, software, and communication protocols. Identify vulnerabilities, potential points of failure, and areas for optimization. This will include the review of:

1. Network administration control
2. Hardening of systems, switches and routers
3. Patch update Management
4. Port based security controls
5. Process control for change management
6. Security incident and management
7. Access control for DMZ application
8. Control filtering for web access and data leakage
9. Password cracking
10. Intrusion detection system testing
11. Router testing

12. Denial of Services testing
13. Review of appropriateness of the network topology
14. Review of adequacy or otherwise of the hardware installed.
15. Network stress / Load test
16. Network Information Security and Administration (Authentication, Access control, operating system controls etc.) of Key Applications Assessment (ATM, Internet Access, Anti-Virus, E-mail, etc.)

iii. Data Centre - CBS Operations

The scope of this engagement encompasses a comprehensive IT audit that will thoroughly assess and evaluate the information technology systems, security protocols, and compliance measures at AUB, including a specific focus on the Data Centre - CBS Operations. The selected vendor will be responsible for the following key areas:

(1) Audit of Data Centre operations for Core-Banking

- Physical Security

a) Physical access controls.
b) Environment management systems such as electrical supply, UPS, air conditioning, fire detection and suppression, generator, etc.

- Operating System (OS)

a) Set up and maintenance of operating system parameters.
b) Updating of OS Patches.
c) OS Change Management Procedures.
d) Use of root and other sensitive passwords.
e) Use of sensitive system software utilities.
f) Interfaces with external applications.
g) Monitoring and Alert management procedures.

(2) Application Software – Core Banking Solutions (CBS and Related interfaces)

a) Authorization Control such as concept of maker checker, exceptions,
overriding exceptions, and error conditions.
b) Authentication mechanism.
c) User Management & Password Management.
d) Parameter Maintenance.
e) Access rights.
f) Access logs/ Audit Trail generation.
g) Change management procedures including procedures for testing.
h) Documentation of change management.

(3) DBMS and Data Security:

a) Secure use of DB and Interfaces.
b) Control procedures for changes to the parameter files.
c) Logical access controls.
d) Control procedures for sensitive database passwords.
e) Control procedures for purging of Data Files.
f) Procedures for data backup, restoration, recovery and readability of backed up data.

iv. Disaster Recovery and Business Continuity Analysis

Evaluate the bank's disaster recovery and business continuity plans, including backup and recovery procedures. Verify the effectiveness of these plans through simulated scenarios and recommend improvements. These will include:

1. Compliance with Bank's Disaster Recovery Plan aspects
2. Log shipping/data sync/archival management
3. Systems high availability and redundancy

Review the Disaster Recovery Plan/Procedures documented for Core Banking Solution and its implementation by the bank at the Data Centre and Disaster Recovery Centre.

v. IT Products

1) ATM and Card Operations and Reconciliation:

Audit of ATM card operational processes with respect to

a) PIN Management
b) Card Management
c) Delivery of ATM cards/ PINs to customers
d) Customer dispute resolution
e) Reconciliation within the Bank and with settlement agency/Banks
f) ATM Network and physical security Architecture Analysis
g) ATM functionality audit
h) ATM Switch
i) Vulnerability analysis of ATM Network
j) Analysis of administrative procedures
k) Outsourcing arrangements and third-party applications
l) ATM sharing arrangements with other Banks/Master/Visa and other agencies and compliance thereof.

2) Internet/Mobile Money:

a) To Assess Flaws in Web hosting i.e Security of web server and Design of the Applications.
b) Attempting to guess passwords using password-cracking tools.

c) Search for back door traps in the site.
d) Attempting to overload the systems using Distributed Denial of Services (DDOS) and Denial of Services (DOS) attacks.
e) Attempting penetration through perceivable network equipment/addressing and other vulnerabilities.
f) Check Vulnerabilities like IP Spoofing, Buffer Overflows, session hijacks, account spoofing, Frame Spoofing, Caching of web pages, Cross site scripting, Cookie handling, injection flaws
g) 256-bit SSL Certificate & PKI verification.
h) To check whether servers are updated with latest security patches.
i) Confirm Rule base in Firewall are configured properly.
j) To ascertain IDS is configured for intrusion detection, suspicious activity on host are monitored and reported to server, firewall and IDS logs are generated and scrutinized. IP routing is disabled.
k) Proxy Server is issued between Internet and proxy systems.
l) Vulnerabilities of unnecessary utilities residing on Application server.
m) Computer Access, messages are logged and security violations reported and acted upon.
n) Effectiveness of Tools being used for monitoring systems and network against intrusions and attacks.
o) Any other items relevant in the case of security.

3) Non-Core Banking Units (Domain Controllers, Endpoint Security Solutions, Windows Update Services, Users Workstations)

a) Domain controller setup, changes, security, availability, function and daily operations control and monitoring.
b) Endpoint security solution, operation and daily monitoring procedures and control.
c) Windows update services deployment methods, controls and operations.
d) User workstations review and control procedures.

vi. Vulnerability Assessment and Penetration Testing

Perform thorough vulnerability assessments and penetration testing to identify potential weaknesses and security breaches. Test the bank's defenses against external threats and internal vulnerabilities.

Though the relevant areas for the penetration testing is already defined especially for the web based applications however this area needed to be covered based on the discussion and suggestions and finding by the Audit firm specifically.

vii. Data Security and Access Control Evaluation

Examine data protection measures, encryption protocols, and access controls within the Data Centre - CBS Operations. This includes evaluating the bank's methods of granting, managing, and monitoring access to critical systems, applications, and sensitive data.

viii. Regulatory Compliance Review

Audit the bank's adherence to relevant industry regulations and standards, including those specific to the Data Centre - CBS Operations. Provide a comprehensive assessment of compliance gaps and recommendations for alignment.

Based on the contents of the RFP, the selected audit firm shall be required to independently arrive at Audit Methodology, based on globally acceptable standards and best practices. The Bank expressly stipulates that the audit firm selection under this RFP is on the understanding that this RFP contains only the principal provisions for the entire audit assignment. The audit firm shall be required to undertake to perform all such tasks, render requisite services and make available such resources as may be required for the successful completion of the entire audit assignment at no additional cost to the Bank.

9. Audit Approaches

Information Systems Audit approach includes the following:

Auditing around the systems.
Auditing through the systems.
Auditing with the systems.

Based on the audit findings risk assessment to be classified as Low, Medium, High, Very High and Extremely high in each specific audit areas.

10.Audit Methodology

The audit work will include manual procedures, computer assisted procedures and fully automated procedures, depending on the chosen audit approach.

11.Reporting and Documentation

Provide a detailed and comprehensive audit report that includes findings, risk assessments, and actionable recommendations for each assessed area. Ensure clear and concise documentation of audit procedures, methodologies, and results.

Risk analysis along with Risk Matrix with scoring model should be submitted as part of audit findings.
Audit firm shall deliver detailed reports as below:

1. Audit (Technical & Process) Report of all the areas covering the objectives, efficiency and effectiveness
2. Presentation to the Top Management of the findings of the Reports
3. Risk Analysis Report.
4. Working papers.
5. Recommendations for Risk Mitigation
6. Gap analysis and recommendation for mitigation
7. The check list with guidelines for the subsequent audit (hard & soft copies)

8. The report findings should cover all the areas separately mentioned in the scope.

12.Timeline

The entire audit should be completed within 1 month from the date of letter of appointment.

13.Pre-Qualification Criteria

The audit firm is required to meet the following minimum eligibility criteria and provide adequate documentary evidence for each of the criteria stipulated below:

1. Relevant Experience and Expertise:

- Demonstrated experience in conducting IT audits for financial institutions, particularly banks.

- Expertise in evaluating complex network infrastructures, data security measures, and compliance requirements.

2. Team Composition and Qualifications:

- Qualifications, certifications (CISA/CISSP/CISM/ITIL Expert), and relevant experience of key team members involved in the engagement.

- Ability to demonstrate a deep understanding of IT audit practices and financial sector regulations.

3. Cost Proposal:

- Competitive and transparent cost estimate for the IT audit, including all associated fees and expenses.

- Value proposition in relation to the quality of service offered.

4. Quality of Previous Work:

- Successful track record of delivering high-quality IT audit services to financial institutions in Afghanistan.

- References and case studies showcasing positive outcomes and client satisfaction.

14.Professionalism

The audit firm should provide professional, objective and impartial advice at all times and hold the Bank's interest's paramount and should observe the highest standard of ethics while executing the assignment.

15.Adherence to Standards

The audit firm should adhere to laws of land and rules, regulations and guidelines prescribed by various regulatory, statutory and Government authorities.

16.Audit Firm Selection/Evaluation Process

The Technical Proposal will be evaluated first for technical suitability. Commercial Proposal shall be opened only for the short-listed bidders who have qualified in the Technical Proposal evaluation.

17.Submission of Bids:

The bids shall be in two parts. Technical Proposal and Commercial Proposal. Both Technical and Commercial Bids shall be submitted in email to the following email.

Subject: Proposal for IT Audit Full Scope: RFP: Number
Email: itaudit@afghanunitedbank.com

Proposals must be submitted to the above-mentioned address no later than 31-Jan-2025.
Bids/Proposals received after the due date will not be considered further.