RFP	AUB/IT/0038
Subject	Proposal for IT Audit Full Scope
Issue Date	18-Jun-2019
Closing Date	08-Jul-2019

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) and received incorporation license from Afghanistan Investment Support Agency (AISA). The Bank is currently operating through 24 branches in Kabul, Nangarhar, Kandahar, Balkh, Herat, Kunduz, Parwan, Helmand, Nimroz, Khost and other big cities of the country. The bank is offering financial products and services in both Conventional and Islamic Banking across these branches.

PROJECT SUMMARY:
Afghan United Bank is seeking all qualified Audit companies (preference will be given to IT Audit specialized Companies) to participate and provide their best proposal for the AUB IT Full Scope Audit.

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 AISA or Ministry of Commerce license whereas the foreign located partners'/vendors companies bidding for this RFP shall include 7% tax and the mentioned percentage will be deductible upon invoice payment.

GOVERNMENT LICENSE & BANK ACCOUNTS:
Before the signing of the Agreement, the company shall provide a copy of the organization's AISA or Ministry of Commerce license and TIN (Tax Identification Number). Foreign companies shall also submit the country issued license.

Company is required to have the Bank account with account details provided on the Bank letter head provided by the Bank having account with.

PROPOSAL CURRENCY:
The proposal currency should be USD whereas the transfer will be made if Local in Afghani considering the day Central Bank Ex Rates and for foreign companies the transfer will be made either in AED/EUR/INR.

SIMILAR CONTRACTS:
Companies are required to provide the proof of the implementation of similar contracts. Afghan United Bank based on the requirement will contact the organizations for the legitimacy of the provided proofs.

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.

CURRENT RFP OBJECTIVES:

1.1 Audit Objectives:

The Bank wishes to appoint competent audit company for conducting an Audit of its IT complete architecture, policies, Security architecture and rest of the infrastructure with the major objectives of evaluation of internal system and control for

Safeguarding of Information System
Assets/Resources Maintenance of Data
Integrity, Reliability and Confidentiality
Maintenance of System Effectiveness
Ensuring System Efficiency

1.2 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.

1.3 Audit Methodology:

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

1.4 Auditors:

Audit should be carried out by Certified audit firm and the certified persons having **CISA/CISSP/CISM/ITIL Expert** qualifications with adequate experience in the audit areas given below and specifically from technical point of view, the firm itself and the Auditor should be well aware of the Core Banking Setups and having good knowledge of **Oracle Databases, Oracle Solaris, Oracle Weblogic and Oracle Financial experience** will be highly preferred.

1.5 Audit Scope:

A description of the envisaged 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 Bank groups the entire proposed audit into following major areas as under

a. Audit of Information Security Architecture & Implementation of Information Security Policy
b. Data Centre - CBS Operations
c. Disaster Recovery Site – BCP
d. IT Products
e. Penetration Testing (Internal & External)
f. Operation Technical Workflow & Procedures

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.

1.6 Audit Findings & Reports:

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:

The following reports are an indicative that should be covered for the area-wise auditing-

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) Recommendations for Risk Mitigation
5) Gap analysis and recommendation for mitigation
6) The check list with guidelines for the subsequent audit (hard & soft copies)

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

1.7 Duration of Audit:

The entire audit should be completed within 45 working days from the date of letter of appointment.

1.8 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:

The audit firm should be in existence for a period of at least 3 years
The audit firm should be a profit-making company in the last 2 years
The audit firm should have a pool of resources (minimum of five experts) who possess qualifications such as **CISA/CISSP/CISM/ITIL Expert/Oracle DB-WebLogic/Oracle Financials**

The audit firm shall be in computer Audit Business for the past 5 years and should have done the Information system Audit of a Core Banking and financial systems Project Audit in a Public Sector bank / Large Private Sector Bank.

The audit firm should not be involved directly or indirectly in implementing CBS Project of the Afghan United Bank

1.9 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.

1.10 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.

1.11 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.

1.12 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

1.13 Scope of Audit:

The details provided in the scope are indicative lists but not restricted to the following.

Area 1: Audit (Technical & Functional):

1) Audit of Information Technology Policies, Environment and SLAs:

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

2) Audit of key IT Systems and Resources

Network Management & Security Audit:

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.)
17. The Bank's WEB-site and servers

Area 2: Data Centre - CBS Operations:

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

(1) Physical Security

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

(2) 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 – Oracle Financials (CBS and Other interfaces, if any)

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 Oracle 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.

Area 3: Disaster Recovery Site - BCP:

Audit of DR Site with respect to

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

Area 4: 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.

Area 5: Penetration Testing:

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.

Area 6: Operation Technical Workflow & Procedures:

Audit of Operation Technical Workflow and business process application controls/ procedures involving the Cash Transactions, Customer Data Gathering, Policies governing the operation technical procedures, System Reporting & Reconciliation procedures.

PROPOSAL SUBMISSION:

Proposals must be submitted to the above-mentioned address no later than 08 July, 2019 – 3:00 PM.
Bids/Proposals received after the due date will not be considered further.

Request bidders' information as per the format attached (Annexure 1), the document also contains the modules list at the second page.

Annexure 1: Audit Firm Information

1. Name
2. Constitution and year of establishment
3. Registered Office/Corporate office/Mailing Address
4. Names & Addresses of the Partners if applicable
5. Contact Person(s):
6. Telephone, Fax, e-mail
7. Number of CISA/CISSP/CISM/ITIL /Oracle DB-WebLogic/Oracle Financials Qualified/ BS7799 lead auditors/ ISO 27001 persons who would be involved in the Audit work along with names and experience.
8. Qualified network professionals who would be involved in the Audit work, if required.
9. Proof of experience in CBS System Audit. Please give details of the same including the details of services and the scope.
10. Describe Project Management methodology for the proposed CBS System Audit assignment, clearly indicating about the composition of various teams.
11. Describe Audit Methodology and Standards to be used for CBS System Audit
12. Indicate Project Plan with milestones and the time frame of completion of different activities of the audit.
13. List of Deliverables as per the „Scope of Work".
14. Specify that technical consultants who would be involved in the Audit work be certified on types of tools used for audit.
15. Details of the biggest Information Security Audit including the scope, service cost and details of services in last 3 years.
16. Any other related information, not mentioned above, which the Audit Firm wish to furnish.

Solutions & Modules (licensed) Pertaining to Area 6:

- AML from Virmati Software
- Acuity Screen Solution
- Oracle FCUBS Banking Base
- Oracle FCUBS Banking Fund Transfer
- Oracle FCUBS Banking Electronic Messaging
- Oracle FCUBS Banking Cash Management (Teller Module and Vault Management)
- Oracle FCUBS Banking Bills and Collections
- Oracle FCUBS Banking Letter of Credit
- Oracle FCUBS Banking Foreign Exchange
- Oracle Flexcube Integration Gateway
- Oracle FCUBS Banking Current and Saving Accounts (CASA)
- Oracle FCUBS Banking Term Deposit
- Oracle FCUBS Banking Consumer Loans (CL)
- Oracle FCUBS Banking Standing Instruction
- Oracle FCUBS Banking Branch
- Oracle FCUBS Banking ATM Interface
- Oracle FCUBS Banking POS Interface
- Oracle FCIB Base
- Oracle FCIB Term Deposit
- Oracle FCIB Islamic Financing
- Oracle FCIB Islamic Profit
- Oracle FCIB Letter of Credit
- Oracle FCIB Current and Saving Accounts