The First Microfinance Bank Afghanistan (FMFB-A)

Request for Proposal
For
Penetration Testing and Audit

Version: 1.0.0
Date of Issue: 14/12/2020

Privacy Notice
This document contains sensitive information owned by FMFB-A Afghanistan. The information, in part or full or in any circumstances, should not be given to persons other than those involved in the project or who will become involved during the project lifecycle. The

prior written permission of Project Manager shall be needed to share full or partial information with the persons or organizations other than the legal / authorized recipients.

Table of Contents

1. Statement of Work

1.1 Purpose

The purpose of this Request for Proposal (RFP) is to invite prospective Bidders to submit a proposal for carrying IT security assessment, penetration testing and IT audit for the year 2020.

1.2 Coverage and Participation

The intended coverage of this RFP, and any agreement resulting from this solicitation, shall be for the use of all departments at FMFB-A. FMFB-A reserves the right not to enter into any contract, to add and/or delete elements, or to change any element of the agreement and participation at any time without prior notification and without any liability or obligation of any kind or amount.

2. General Information

2.1 Original RFP Document

FMFB-A shall retain the RFP, and all related terms and conditions, exhibits and other attachments, in original form in an archival copy. Any modification of these, in the vendor's submission, is grounds for immediate disqualification.

2.2 The Bank

The First Microfinance Bank, Afghanistan has been operating as Commercial Bank registered with Da Afghanistan Bank (DAB) with the vision to be recognized as the leading microfinance services provider in Afghanistan contributing to poverty alleviation and economic development through the provision of sustainable financial services primarily targeting at the micro & small businesses and households. This vision lays tremendous responsibility for the bank to ensure its operations continued effectively, providing all banking solutions to its customers. In this regard, amongst many other facilities FMFB-A provides the Online Transactions service to it valued customers.

2.3 Schedule of Events

The following is a tentative schedule that will apply to this RFP, but may change in accordance with the organization's needs or unforeseen circumstances. Changes will be communicated by e-mail to all invited bidders.

Issuance of RFP	14/12/2020
Final Award Notification	29/12/2020

3. Proposal Preparation Instructions

3.1 Bidder's Understanding of the RFP

In responding to this RFP, the Bidder accepts the responsibility to fully understand the RFP in its entirety, and in detail, including making any inquiries to FMFB-A as necessary to gain such understanding. FMFB-A reserves the right to disqualify any Bidder who demonstrates less than such understanding. Further, FMFB-A reserves the right to determine, at its sole discretion, whether the vendor has demonstrated such understanding. That right extends to cancellation of award prior to contract signing, if an award has been made. Such disqualification and/or cancellation shall be at no fault, cost, or liability whatsoever to FMFB-A.

3.2 Good Faith Statement

All information provided by FMFB-A in this RFP is offered in good faith. Individual items are subject to change at any time. FMFB-A makes no certification that any item is without error. FMFB-A is not responsible or liable for any use of the information or for any claims asserted there from.

3.3 Communication

Verbal communication shall not be effective unless formally confirmed in writing by the specified procurement official in charge of managing this RFP process. In no case shall verbal communication govern over written communication.

3.3.1 Vendors' Inquiries. Applicable terms and conditions herein shall govern communications and inquiries between FMFB-A and Bidders as they relate to this RFP. Inquiries, questions, and requests for clarification related to this RFP are to be directed in writing to:

FMFB-A
IT Department/ Head Office, Kabul
Lane 8, Kolola Pushta Road, District 4,
Shahr-e-Naw, Kabul - Afghanistan.

3.3.2 Informal communications shall include, but are not limited to: requests from/to Bidders or Bidders' representatives in any capacity, to/from any FMFB-A employee or representative of any kind or capacity with the exception for information, comments, speculation, etc. Inquiries for clarifications and information that will not require addenda may be submitted verbally to the above named at any time.

3.4 Proposal Submissions

Proposals must be delivered sealed to:

FMFB-A
PSD Department/ Head Office, Kabul
Lane 8, Kolola Pushta Road, District 4
Shahr-e-Naw, Kabul - Afghanistan

To: Muhib Kabiri
Procurement Manager
+93790008103
Muhib.kabiri@fmfb.com.af

Vendors are to submit one (1) original copy of proposal marked "Original" and one (1), marked "Copy." Each original and copy must be individually bound.

3.5 Method of Award

The evaluation of each response to this RFP will be based on its demonstrated competence, compliance, format, and enterprise. The purpose of this RFP is to identify those vendors that have the interest, capability, and financial strength to supply FMFB-A with the following Scope of Work.

Following will be Evaluation Criteria but not limited to:

1. Capability of vendor to meet or exceed requirements set forth in Scope of Work.
2. Expressed interest in working with FMFB-A.
3. Financial stability of vendor.
4. Ability of vendor to communicate its vision and capacity for establishing a relationship that addresses current and future needs and trends in the industry.
5. Desirability of proposed solution.
6. Cost effectiveness

3.6 Selection and Notification

Bidders determined by FMFB-A that possess the capacity to compete for this contract will be selected to move into the negotiation phase of this process. Written notification will be sent to these vendors via mail. Those vendors not selected for the negotiation phase will not be notified.

4. Scope of Work, Specifications and Requirements:

The purpose of this RFP is to identify the qualified bidders to help FMFB-A to conduct an audit of its IT complete architecture, policies, security architecture, other IT infrastructures, vulnerabilities, Risk associated with IT infrastructures and business applications such as Online Banking Infrastructure, Core Banking and FMFB public Network Infrastructure. In additions the security Risk Assessment, the Qualified bidder shall also conduct the IT audit for the year 2020.

4.1 In-Scope Applications, Devices, Services and Components

- **Core Banking**
  - Database Server
    - Oracle DB and Interfaces Security
    - Control procedures for changes to the parameter files.
    - Logical access controls.
    - Procedures for sensitive database passwords.
    - Procedures for purging of Data Files.
    - Procedures for data backup, restoration, recovery and readability of backed up data.
  - Application Server
    - Access Control with maker checker concept, and errors.
    - Authentication mechanism.
    - User Management & Password Management.
    - Parameterizations.
    - Access rights.
    - Access logs/ Audit Trail generation.
    - Change management procedures.
    - Documentation of change management.
    - Integration of Core banking system with other systems
    - Review of core banking transactions and validity.

- **Online Banking**
  - Database Server
  - Application Server
  - Web Server
- **Network**
  - Switches
  - Routers
  - Firewalls
  - Wireless Network (Access points)
  - Port security
  - Intrusion detection systems and Event management.
  - Review of network topology correctness
  - Network device adequacy and redundancy test.
  - Network load test.
  - FMFB-A website security assessment
- **Disaster Recovery Site**
  - Business Continuity plan (BCP)
    - Disaster Recovery plan execution methods.

- Log file movement, data synchronization to DR site and data archives methods.
- Core applications high availability test and redundancy analysis

- **Information security Systems**
  - Data Encryption over network and Systems
  - Data back up and restoration procedure review

- **Operating Systems**
  - Set up and maintenance of operating system parameters.
  - Updating of OS Patches.
  - Use of root and other sensitive passwords.
  - Use of sensitive system software utilities.
  - Interfaces with external applications.
  - Monitoring and Alert management procedures.

- **Datacenter Management review**
  - Physical security review
  - Environmental review of power supply (UPS, power redundancy, cooling system, surveillance, fire alarm systems, smoke detections systems and generators).
  - Physical access authentications mechanism and control review

- **IT services and Products**
- **Penetration testing both (Internal and External)**
  - Verification and validation of security certificates and PKI verification
  - Attempt to overload the servers and applications with Distributed Denial of Services (DDOS) and Denial of Services (DOS) attacks.
  - Check Vulnerabilities like IP Spoofing, Buffer Overflows, session hijacks, account spoofing, Frame Spoofing, Caching of web pages, Cross site scripting, Cookie handling, injection flaws.
  - Testing of password complexity and guess password using cracking tools.
  - Proxy Server configuration and assessment.
  - Vulnerabilities of unrequired configs, files and utilities used and residing on Application servers.
  - To check availability of logs monitoring, event management, monitoring systems and reporting of network intrusions and suspicious network traffic monitoring.
  - Verification and authentication of other flaws and systems and devices weaknesses.

- **ATM Network security and vulnerability assessment and remediations.**
- **Vendor SLAs and Service Agreements.**
  - Contract management
  - Technical support availability

- **Internet accessibility, monitoring and filtering procedures and security flaws assessment.**
- **Assessment of all single point failures of connections, VPN setup, Security mechanisms, redundancy and firewall rules set up.**
- **Patch Management, System configuration hardening process assessment.**
  - Domain controller set up and configuration assessment and operations.

- Endpoint security solution, operation and daily monitoring procedures and control.
- Windows update services deployment methods, controls and operations.
- User workstations review and control procedures.

- **IT Policies and Procedures review**

4.2 Risk Assessment:

The service provider shall conduct the risk assessment of the in-scope infrastructure and application for any risks that is associated and can lead to threats and data loss for the FMFB or affect the Confidentiality, Integrity and Availability of information in the organization. This will include the review of the current setup, configuration and suggestion based on the best practices.

4.3 Vulnerability assessment:

The objective of vulnerabilities assessment is to identify and determine the threats faced by FMFB-A services and internal hosts. The service provider shall conduct vulnerability assessment for the in-scope applications and infrastructure and help the bank to identify the vulnerabilities associated with these services and infrastructure. The service provider shall document and submit the final executive and detailed reports with categorization of the vulnerabilities based on the risk level, impact and exposure.

4.4 Exploitation & Escalation:

The service provider shall exploit using the vulnerabilities identified as result of the vulnerability assessment to obtain the un-authorized access, code injections, and using other methodologies for un-authorized access and breach. In addition, the service provider shall also attempt for escalation. This will help the bank to identify the dept of the vulnerably, security breach and the exposure to the real attack. The service provider shall submit the result of the exploitation and escalation to FMFB-A and the action and control to mitigate those vulnerability in the risk response plan.

4.5 Risk Response Plan:

Once the risk assessment is completed, the service provider shall submit the risk response plan that will identify the actions and controls to be undertaken to mitigate and address the risk. The Document shall clearly state the Risk, impact, control and the responsibility of parties. All the actions and controls must be appropriate for the organization in terms of cost, feasibility and should be as per FMFB-A policy.

4.6 Audit Year 2020

The service provider or auditor shall conduct the IT audit for FMFB-A Information Technology department for the year 2020. The Auditor shall commence the audit based on the international auditing standards with generally accepting auditing standards and procedures. The objective of this audit to ensure the IT operations are with accordance to the defined policies and procedures

5. Methodology and Approach:

The service provider shall include the methodologies and the approach they will be using for the security assessment and the penetration testing.

- ✓ How the Security assessment will be carried out
- ✓ The activities that will be carried out form within FMFB-A network or from outside
- ✓ Tool to be used for the security assessment and exploitation
- ✓ How the simulated attack and penetration testing will be carried out
- ✓ Expectation and responsibilities of FMFB-A IT department.

Approaches:

- ✓ Audit Around the system
- ✓ Auditing through the system
- ✓ Auditing with the system

6. Experience and Qualification:

Only those bidders, who fulfill the following criteria are eligible to respond to this RFP, Bids received from the bidders who do not fulfill any of the following eligibility criteria are liable to be rejected

- ✓ The bidder should be legal entity registered in Afghanistan or internationally
- ✓ The bidders must have at least fiver years of experience in related field. IT Audit and IT security assessment and penetration testing
- ✓ The bidders must have qualified and experienced resource to conducted IT Security assessment and Audit
- ✓ The bidders must be able to provide at least client references for whom similar projects carried out
- ✓ The bidder must provide the certification and profile of their staff whom will be engaged in the assignment
- ✓ The bidder should have experience of technical expertise in management of IT systems and expertise with (Oracle database, Solaris, Oracle weblogic and Financial systems and configuration management).

7. Proposal Currency:

All the cost and prices should be in the USD and in case of the local company the transfer will happen in Afghani while for the international companies the transfer will happen either in USD or EUR

8. Timeline:

The timeline for this project should be clearly stated and the number of days or weeks required for each phases of this engagement. Also, the service provider should state the number resource engaged onsite and remote and the time required to issue the final report

9. None Disclosure Agreement:

The winner for this bid shall sign Non-Disclosure Agreement with FMFB-A prior starting the project.

10. Bidder Certification:

This certification attests to the Bidder's awareness and agreement to the content of this RFP and all accompanying calendar schedules and provisions contained herein.

The Bidder must ensure that the following certificate is duly completed and correctly executed by an authorized officer of your company.

This proposal is submitted in response to RFP issued by FMFB-A. The undersigned is a duly authorized officer, hereby certifies that:

_____

(Bidder Name)

agrees to be bound by the content of this proposal and agrees to comply with the terms, conditions, and provisions of the referenced RFP and any addenda thereto in the event of an award. Exceptions are to be noted as stated in the RFP. The proposal shall remain in effect for a period of thirty (30) calendar days as of the Due Date of the RFP.

The undersigned further certify that their firm (check one):

□ IS
□ IS NOT

currently debarred, suspended, or proposed for debarment by any Govt./other entity. The undersigned agree to notify FMFB-A of any change in this status, should one occur, until such time as an award has been made under this procurement action.
Person(s) authorized to negotiate on behalf of this firm for purposes of this RFP are:

Name: _____ **Title:** _____

Signature: _____ **Date:** _____

Name: _____ **Title:** _____

Signature: _____ **Date:** _____

Signature of Authorized Officer:

Name: _____ **Title:** _____

Signature: _____ **Date:** _____