VULNERABILITY ASSESSMENT PENETRATION TEST

1. INTRODUCTION

Financial Sector Deepening Kenya (FSD Kenya) is an independent trust dedicated to the achievement of a financial system that delivers value for a green and inclusive digital economy while improving financial health and capability for women and micro and small enterprises (MSEs).

We work closely with the public sector, the financial services industry, and other partners to develop financial solutions that better address the real-world challenges that low-income households, micro and small enterprises, and underserved groups such as women and youth face.

FSD Kenya was established in 2001 to support the development of inclusive finance to stimulate wealth creation and to reduce poverty. In 2005, FSD Kenya was constituted as an independent trust. We operate under the supervision of professional trustees with policy guidance from a programme investment committee (PIC).

Our current funders are FCDO, the Swedish International Development Cooperation Agency (SIDA), and the Bill & Melinda Gates Foundation.

2. OBJECTIVES

FSD Kenya wishes to appoint a consultant to conduct vulnerability assessment and penetration testing ("VAPT"), security posture review and cybersecurity awareness training.

2.1 Project context

FSD Kenya has implemented various information systems in a bid to improve efficiency and effectiveness in the delivery of its mandate. To ensure that the information systems are safeguarding our assets, maintaining data confidentiality, integrity, availability and operating at optimum levels, FSD Kenya requires the consultant to conduct vulnerability scanning, penetration testing and review of our logical security perimeter, as well as provide cybersecurity-awareness sessions for all FSD Kenya staff members.
The testing process should follow standard methodologies such as target identification, enumeration, vulnerability assessment, exploitation attempt, clean-up, and reporting. The testing must be non-destructive and non-intrusive. FSD Kenya should not experience DDOS (Denial of Service attacks), Data loss & destruction and lost time or access impairment in the delivery of this project. The training should be inclusive, with proof provided that all staff have been trained, and certificates provided on completion.

Based on known, consensus best practices, and a wealth of practical experience and expertise from the technology industry, this exercise will provide the education and guidance needed to understand and improve FSD Kenya's information security posture.

The objective is to carry out a comprehensive review and examination of information communication and technology assets at FSD Kenya. This will involve evaluating the system's internal control design and effectiveness and an examination of the network perimeter,

internal security posture, system security, database security, and cloud operation's security The consultant shall report on the conclusions reached from its review of the systems and recommend suitable measures for correcting any deficiencies which were identified during the process. At the end of this exercise, FSD Kenya will have identified areas that need improvement and enable us to make relevant updates to the FSD Kenya Information Security infrastructure. In addition, it will enable FSD Kenya to measure the feasibility of its systems or end-user.
compromise, as well as evaluate any related consequences such as incidents that may arise and involve resources or operations. FSD Kenya is then able to measure the security and resilience of its systems, and level of the cyber threat to its end users. During the exercise, the consultant will be required to work with the IT staff to ensure that the exercise is carried out successfully by following all required steps.

3. SCOPE OF WORK

The areas of focus on this exercise include but are not limited to:

3.1 Vulnerability assessment

1. Anonymous information gathering to discover all Internet-facing assets a hacker could identify as potential entry-points into the organisation's network and infrastructure.
2. Scanning of internet-available servers and web services for known vulnerabilities.
3. Verifying scan-result findings through in-depth manual penetration testing attack techniques.
4. Providing deeply informed remediation guidance and advisory services for identified/verified vulnerabilities.
5. External and internal network vulnerability assessment and penetration testing.
6. Internal web application penetration testing.
7. Server security and configuration reviews.
8. Database security and configuration reviews.
9. Third party interconnection reviews such as bank integration, vendor database, API reviews etc
10. Application security configuration reviews for systems such as Dynamics 365 and portals.
11. System configuration and change management reviews.
12. Access, authorisation, and session management testing for all users and administrators
13. Denial of service testing.
14. Data validation testing.
15. Cloud firewall and virtual network configuration reviews and testing.
16. Cloud environment security assessment.
17. VPN configuration reviews – S2S and P2S VPNs.
18. Intrusion detection/prevention system testing- Kaspersky Cloud security
19. Password service strength testing.
20. Email security testing such as phishing and malware control
21. DR testing such as backup and restore, redundancy and environment segregation.
22. Office 365 FSD Kenya configurations vulnerabilities
23. SharePoint segregation of duties and rights assignment
24. Security audit on Office 365 security groups.

3.2 Security training

Train FSD Kenya staff on cybersecurity awareness

4. CONDUCT OF THE WORK

Target identification
In this planning and reconnaissance stage, the consultant and the FSD Kenya IT staff will define the scope and goals of the tests. This will include the systems to be accessed and testing methods to be used. In this case the systems to be addressed will be servers and cloud infrastructure.

The consultant will be gathering intelligence to better understand how a target works and its potential vulnerabilities. FSD Kenya's IT team will provide any required documentations/information such as internet protocols (IPs) to the winning bidder.

Scanning & Enumeration
The next step is to understand how the target application will respond to various intrusion attempts providing a real-time view into an application performance. All services that will be tested should be enumerated at this stage.

Vulnerability assessment & gaining access.
This stage uses web application attacks, such as cross-site scripting, SQL injection and backdoors, to uncover the target's vulnerabilities. The testers try to exploit these vulnerabilities, typically by escalating privileges, stealing data, intercepting traffic, etc., to understand the damage they can cause.

Exploitation & Maintaining access.
The goal of this stage is to see if the vulnerability can be used to achieve a persistent presence in the exploited system— long enough for a bad actor to gain in-depth access. The idea is to imitate advanced persistent threats, which often remain in a system for months to steal an organisation's most sensitive data.

Report and Analysis
The consultant will be required to give a report on the exercise, which outlines key objectives and findings such as: Specific vulnerabilities that were exploited, sensitive data that was accessed, the amount of time the penetration tester was able to remain in the system undetected. The consultants will also be required to develop a roadmap showing the recommended controls to be implemented to resolve gaps identified during the penetration test engagement. The roadmap will
be built upon an agreed timeline. Individual analysis report will be provided for each firewall, standalone device, and system.

Training & Presentation of findings
A presentation of key findings will be presented to the FSD Kenya team which summarises the findings documented in the report. Training on impact and how to carry out remediation will be conducted for all FSD Kenya IT staff.
All FSD Kenya employees will receive two graded cyber-security awareness training sessions.

Topics that will be covered in each of the cybersecurity awareness training sessions are not limited to;

- Phishing, malware, and ransomware
- Password security
- Removable media, Encryption and Backup
- Social Engineering and social media
- Bowser and Mobile security
- Incident reporting, response, and management
- Wifi- Public and corporate wifi
- Privacy, Multifactor authentication, Single-sign-on

5. OUTCOMES AND DELIVERABLES

The consultant is expected to deliver.

- Inception report within two weeks of signing of contract.
- Penetration test report with detailed recommendation and action plan.
- User awareness training
- Report & Handover. The contracted firm is expected to provide an actionable report with detailed findings and appropriate recommendations as well as an implementation plan agreed on with Management to correct the deficiencies.

The copyright for all material prepared under these terms of reference will pass to FSD Kenya. It is FSD's practice to publish the reports it commissions in its own house style. There is therefore no requirement for material to be extensively formatted beyond that required to indicate how material should be logically presented in the final report. All final reports should be presented in an electronic format allowing the text and graphics to be manipulated in preparation for publication. Where a final report is presented in a portable document format (pdf) generated from another format (such as Microsoft Word) it should be accompanied by the original file from which it is generated. All representations of graphic material (tables, figures, drawings, charts, graphs and photographs) must be able to be reproduced at high print resolution. Tables, figures, drawings, charts, graphs should be provided in Microsoft Excel or Adobe Illustrator format. Photographs must be provided in high-resolution JPG images set to minimum of 300 dots per inch (dpi). Any technical questions regarding these requirements should be addressed to FSD's Communications Officer.

6. REQUIREMENTS

FSD Kenya is inviting a proposal from suitably qualified consultants/consultancy firms.

Project Schedule

Provide a detailed schedule showing your work break down, activity sequence, key milestones, and a confirmation of your ability to meet the milestones. You will specify the methods and tools that you will use to measure and monitor effectiveness of the assignment.

Project Cost

An itemised project cost that reference each identified activity / milestone and its associated costs. The budget should cover professional and reimbursable fees, fee rates, number of days and a breakdown of the expenses.

Experience

Please provide a reference to at least three corporate clients who have successfully undergone a similar assignment. Submit contract/Local Service Order/Letter of Award in the English language. You can share recommendation letters from these clients as well of work done in the past 24 months that involved the delivery of Vulnerability assessment, Penetration testing and cyber-security awareness training services. The proposal should contain at least three detailed CVs of the team who will undertake the VAPT & cyber awareness training.

Mandatory requirements
A well-established cybersecurity focused firm with a good track record of working on providing cybersecurity services in Kenya and the wider region
Solid knowledge and demonstrated experience in conducting cybersecurity reviews, vulnerability, and pen testing, providing training and providing actionable insights on the outcome of the reviews.
Ability to turn around the assignment and deliver within the set deadlines
Previous experience in Azure cloud, Office 365 and Dynamics 365 Business central security audit.

7. EVALUATION CRITERIA

Assessment criteria	Weighting (%)
Experience of the Consultant/firm	
A well-established cybersecurity focused firm with a good track record of working on providing cybersecurity services in Kenya and the wider region for at least five years.	10
Solid knowledge and demonstrated experience in conducting cybersecurity reviews, vulnerability, and pen-testing, providing training Solid knowledge and demonstrated experience in conducting cybersecurity reviews, vulnerability, and pretesting, providing training and providing actionable insights on the outcome of the reviews with three letters of reference.	10
Approach and methodology	
Methodology/approach for the assignment as outlined in the Scope including rationale for chosen methodology including methods and tools that will be used.	20
Content, quality, and completeness of the proposal – Demonstratable understanding of the TORs	10
Staff schedule, work and deliverable schedule	
Adequacy of the proposed staff schedule to meet the needs of the ToR	10
Responsiveness of proposed work plan in relation to the ToR	10
Key Professional Personnel Qualification for the Assignment **Note: Bidders to respond in relation to the Key personnel requirement and evaluation criteria in this section**	
Responsiveness of the CVs to the requirements of the ToR	10
Financial Evaluation The formula for determining the financial scores is the following:	20

Assessment criteria	Weighting (%)
FS = S% x LB/BP where: FS = financial score LB = Lowest/Most competitive bid BP= Cost of the bid been considered S% = Percentage score The weights given to the Technical (T) and Financial (F) Proposals are: T = 80% and F = 20%	
Total	**100%**

FSD Kenya will undertake a due diligence assessment and screening of the preferred Bidder to include reference checks. FSD Kenya will share a Third-party screening questionnaire to aid in processing the assessment and screening. FSD Kenya reserves the right to proceed or reject Bidder(s) depending on the outcome of this assessment and consider the next ranked bidder. The findings of this assessment will be kept confidential and used internally for the purposes of this evaluation.

FSD Kenya reserves the right to accept any tender (s) or to reject all tenders at any time. FSD Kenya also reserves the right to cancel this procurement at any point in time prior to award of the contract.

If you would like to lodge a complaint in regard to this procurement process, please write to tenders@fsdkenya.org with the address **vulnerability assessment penetration test**. FSD Kenya procurement team will acknowledge receipt of the complaint in writing within three (3) working days.

During the course of this procurement if you come across any issues of bribery, corruption or wrong doing on FSD Kenya part, please feel free to contact Julius Anyega, FSD Kenya Chief Operations Officer at Julius.Anyega@fsdkenya.org or transparency@fsdkenya.org

8. SUBMISSION

Interested bidders should send proposals by email to tenders@fsdkenya.org on or before **March 20th, 2023, at 17:00HRS (EAT)** with the subject line **"vulnerability assessment penetration test"** If you have any clarification questions, please email us at tenders@fsdkenya.org no later than 8th March 2023. Responses to clarification questions shall be sent on 10th March 2023.

Tender security is NOT required. Issuance of this request for proposals in no way obligates FSD Kenya to award a contract. Applicants will not be reimbursed for any costs associated with their application.

9. TIMETABLE

The penetration testing and vulnerability scanning work will be carried out for a period of two months from the signed contract start date. The consultant will provide two cyber-security awareness sessions, one session at the completion of the contract, and the next, 3-4 months later.