VisionFund RWANDA

P.O. Box 6893

Nyarutarama, Kigali, Rwanda

T3527 (For use in Rwanda only)
E info@vfcrwanda.rw

CALL FOR PROPOSALS

"CONSULTANCY SERVICES FOR VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT)"

1. Background

VisionFund Rwanda (VFR) is a regulated deposit-taking microfinance institution committed to improving the lives of vulnerable children and their families by providing responsible and inclusive financial services. As a member of the VisionFund International network and World Vision Partnership, VisionFund Rwanda leverages financial inclusion as a key enabler of sustainable livelihoods and economic empowerment.

To support its operations, VisionFund Rwanda relies on a robust Information Technology (IT) environment that underpins the delivery of its financial services, supports business operations, and safeguards customer and organizational information. Maintaining the confidentiality, integrity, and availability of these information assets is essential to ensuring business continuity, regulatory compliance, and stakeholder confidence.

As part of its ongoing commitment to strengthening cybersecurity and information security governance, VisionFund Rwanda intends to engage a qualified and experienced cybersecurity firm to conduct an independent Vulnerability Assessment and Penetration Testing (VAPT) of its IT environment.

The assessment is intended to provide an independent evaluation of the organization's cybersecurity posture by identifying security vulnerabilities, assessing associated risks, evaluating the effectiveness of existing security controls, and recommending practical measures to strengthen the overall security and resilience of the IT environment.

The proposed approach and methodology should demonstrate consideration of applicable regulatory and legal requirements governing the financial sector in Rwanda, including relevant directives, guidelines, and cybersecurity requirements issued by the National Bank of Rwanda (NBR), the National Cyber Security Authority (NCSA), the Rwanda Information Society Authority (RISA), and other relevant authorities, where applicable.

2. Objectives of the Assignment

The objective of this assignment is to engage a qualified cybersecurity firm to conduct an independent Vulnerability Assessment and Penetration Testing (VAPT) of VisionFund Rwanda's IT environment.

The assessment is expected to:

- Identify security vulnerabilities and weaknesses within the agreed assessment scope.
- Assess the risks associated with identified vulnerabilities.
- Assess technical and process controls
- Evaluate the effectiveness of existing security controls.
- Validate exploitable vulnerabilities, where appropriate.
- Provide executive and technical reporting
- Provide practical and prioritized recommendations to strengthen VisionFund Rwanda's cybersecurity posture.

3. Scope of Services

The successful bidder shall conduct a comprehensive Vulnerability Assessment and Penetration Testing covering, at a minimum, the following areas:

3.1. Network and IT Infrastructure

Assessment of the organization's network and IT infrastructure, including critical infrastructure components such as **servers, network equipment, security devices, and related supporting services**. The assessment should identify vulnerabilities, configuration weaknesses, and security risks that may affect the confidentiality, integrity, or availability of the organization's IT environment. It shall include but not be limited to:

- External and internal network testing
- Active Directory / Entra ID assessment
- Servers, endpoints, firewalls, VPN, DNS, email and network devices

3.2. Business Applications

Assessment of VFR's critical business applications to identify vulnerabilities, security weaknesses, and risks that could impact the confidentiality, integrity, availability, or reliability of business services and information. This shall take into consideration the following:

- Web applications, mobile applications, APIs (including OWASP API Top 10)

3.3. Database Security

Assessment of databases supporting critical business applications to identify security weaknesses, configuration issues, access control deficiencies, and risks that could compromise the security and integrity of organizational data.

3.4. Security Configuration and Technical Controls

Review of security configurations and implemented technical controls across the IT environment to assess their effectiveness, identify control gaps, and recommend improvements based on recognized industry standards and best practices.

3.5. Overall Security Posture

Provide an overall assessment of VisionFund Rwanda's security posture, highlighting significant risks, priority improvement areas, and strategic recommendations to strengthen the organization's overall cybersecurity resilience.

4. Methodology

The Technical Proposal shall clearly describe the standards, methodologies, frameworks, and tools that will be applied in conducting the Vulnerability Assessment and Penetration Testing. The proposed approach should be based on internationally recognized cybersecurity standards and industry best practices, such as the OWASP Testing Guide, OWASP Top 10, OWASP API Security Top 10, PTES, NIST SP 800-115, MITRE ATT&CK, CVSS, and applicable CIS Benchmarks.

5. Vendor Qualifications

Interested firms should demonstrate:

- ✓ Proven experience in conducting VAPT engagements.
- ✓ Experience in financial institutions or regulated organizations is an added advantage.
- ✓ Qualified professionals with relevant industry certifications such as OSCP, CREST, GPEN, GXPN, OSWE, CISSP, CISM, CEH or any relevant certications.
- ✓ Successful completion of at least three similar assignments within the last five years.
- ✓ Legal authorization to provide the proposed services within Rwanda.

6. Rules of Engagement

Testing windows, emergency contacts, change control, prohibited activities, protection of production services, handling of sensitive information, incident escalation, rollback procedures and NDA requirements.

7. Proposal Requirements

Separate technical and financial proposals including methodology, implementation plan, team CVs, references, assumptions, bidder requirements, licences, insurance, and pricing schedule.

8. Evaluation Criteria

Technical Methodology (25%), Relevant Experience (20%), Team Qualifications (20%), Understanding of Assignment (15%), References (10%), Financial Proposal (10%).

9. Proposal Submission Requirements

Interested bidders shall submit separate Technical and Financial Proposals.

9.1. Technical Proposal

- ✓ Understanding of the assignment.
- ✓ Proposed approach and methodology.
- ✓ Implementation plan.
- ✓ Project team and CVs.
- ✓ Company profile and relevant experience.
- ✓ Documented evidence of similar assignments (Recommendations of Successful Service delivery).
- ✓ Client references.
- ✓ Bidder Requirements from VisionFund Rwanda (Clearly specify any information, documentation, system access, resources, assumptions, dependencies, and other support required from VisionFund Rwanda for the successful execution of the assignment).
- ✓ Business registration documents, (RDB Certificate, Tax Clearance, Applicable licenses/regulatory approvals, and conflict of interest declaration if any)

9.2. Financial Proposal

- ✓ Cost Breakdown.
- ✓ Applicable taxes.
- ✓ Proposed payment schedule, where applicable.

10. Expected Deliverables

The successful bidder shall provide the following deliverables:

10.1. Inception Report

- Understanding of the assignment.
- Confirmed scope of work.
- Agreed implementation schedule.
- Key assumptions and dependencies.

10.2. Execution of the Vulnerability Assessment and Penetration Testing

The successful bidder shall execute the agreed Vulnerability Assessment and Penetration Testing in accordance with the approved methodology and implementation plan. The execution shall include all assessment activities necessary to identify, validate, and assess

security vulnerabilities within the agreed scope while minimizing disruption to VisionFund Rwanda's operations

10.3. Assessment Reports

- Executive Report (High-level summary of key findings, business risks, and strategic recommendations)
- Detailed Technical Assessment Report (Detailed technical findings, supporting evidence, risk ratings, and recommended remediation actions)
- Vulnerability Register (including recommended remediation actions and priority ratings)

11. Engagement Requirements

The successful bidder shall:

• Execute a Non-Disclosure Agreement (NDA) before commencement and maintain strict confidentiality.

• All reports, findings, supporting evidence, working papers, and deliverables shall remain the exclusive property of VisionFund Rwanda.

12. Assignment Duration

Bidders shall propose a realistic implementation schedule for the assignment. VisionFund Rwanda's preferred duration for completion of the engagement is approximately **thirty (30) calendar days** from the agreed commencement date. However, bidders may propose an alternative timeline where justified by their proposed approach, scope of work, or other relevant considerations. Preferred duration: 30 calendar days including re-testing, subject to agreed scope.

13. Submission Procedure

- **Proposal:** The technical and financial proposals must be submitted in separate folders. The technical proposal should include all required documents specified under the Submission Requirements section, while the financial proposal should contain the entire financial offer.
- **Deadline:** Well written bid documents prepared in English will be sent to this email address: info@vfcrwanda.rw with "BID FOR CONSULTANCY SERVICES FOR VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT)" in Subject not later than 17th August 2026 at 11:00 pm

Done at Kigali on 5th August 2026

Grace DUSHIMIMANA

Chief Executive Officer

VisionFund RWANDA
P.O Box 6893 Kigali - Rwanda
Date/Sign: .....