

EXPRESSION OF INTEREST (EOI) PROCUREMENT OF CONSULTANCY SERVICES FOR VULNERABILITY ASSESSMENT AND PENETRATION TESTING SERVICES

1. Background

The Insurance Regulatory Authority (IRA) is a State Corporation established under the Insurance Act, Cap 487 of the Laws of Kenya with the mandate to regulate, supervise and promote development of the insurance industry in Kenya. IRA has implemented various information systems in a bid to improve efficiency and effectiveness in execution of its mandate.

To ensure that the information systems are safeguarding assets, maintaining data confidentiality, integrity, availability and operating effectively and at their optimum so as to achieve the Authority's objectives; we wish to engage a reputable firm to provide Vulnerability Assessment and Penetration Testing (VAPT) services.

2. Objective

The objective is to carry out a comprehensive review and examination of the security posture of the Authority in relation to information system assets. This will involve evaluating the system's internal control design and effectiveness and an examination of the network perimeter, internal security posture, system security and database security.

The firm 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 review process.

3. Scope of services

The areas of review shall include but are not limited to the following:

- i. Anonymous information gathering to discover all Internet-facing assets a hacker could identify as potential entry-points into the organizations network.
- ii. Scanning of internet-available network access points and web servers for known vulnerabilities.
- iii. Verifying scan-result findings through in-depth manual penetration testing attack techniques.
- iv. Providing deeply informed remediation guidance and advisory services for identified/verified vulnerabilities.
- v. Internal & External Penetration Testing in the following areas: -
 - a. External and internal network vulnerability assessment and penetration testing.
 - b. Internal web application penetration testing.
 - c. Review of DMZ and network architecture designs.
 - d. Server security and configuration reviews.
 - e. Database security and configuration reviews.
 - f. Third party interconnection reviews.
 - g. Application security configuration reviews.
 - h. System configuration and change management reviews.
 - i. Authorization and session management testing.
 - j. Denial of service testing.
 - k. Data validation testing.
 - l. Firewall and router configuration reviews and testing.
 - m. Data centre security assessment.
 - n. VPN configuration reviews.
 - o. Intrusion detection/prevention system testing.
 - p. Password service strength testing.
 - q. Email security testing.
 - r. DR testing

Information systems in place

- I. Electronic Regulatory System (ERS) through which regulated entities submit their data. The functionalities of ERS are: -
 - Online submission of returns
 - On-site Inspection
 - Analysis and Report Generation
- II. Integrated Management Information System (IMIS) based on Microsoft Dynamic Navision with the following modules:
 - Procurement and Stores module
 - Customer Relationship Management module
 - Consumer Protection module
 - Human Resource and Administration module
 - ICT Service Desk module
- III. Sage Evolution Accounting System
- IV. Memory Soft payroll system
- V. Teammate Internal Audit Management Software
- VI. Firewall, Antivirus and other cybersecurity solutions
- VII. List of Internet Protocols (IPs) will be disclosed to the winning bidder

4. Eligibility criteria

The Expression of Interest must be accompanied by the consultants' qualifications, professional capabilities and details of experience related to similar consultancy services. Interested firms should provide specific information which will be the basis for prequalification as indicated below:

a) Company Profile:

- i. Contact details of the firm; physical address, phone number and email addresses
- ii. List of the current Directors/Proprietors
- iii. Organization structure of the firm
- iv. Contact person with designation and contact details (physical address, phone number and email addresses)
- v. List of key staff relevant to the assignment and their profile; must be composed of relevant staff with a mix of appropriate expertise.

b) Mandatory requirements

- i. Submit a copy of certificate of incorporation.
- ii. Submit a valid Tax compliance certificate.
- iii. Submit evidence of experience in undertaking similar assignments
- iv. The proposed firm must demonstrate experience in conducting vulnerability assessment and penetration testing.

5. Clarifications

Interested individuals may request for clarification up to Seven (7) days before closing date. Any request for clarification must be sent in writing by paper mail or electronic mail to:

**Manager Procurement,
Insurance Regulatory Authority,
Zep-Re Place, Longonot Road, Upperhill,
P.O. Box 43505-00100
Nairobi, Kenya
Email: procurement@ira.go.ke**

6. Submission

Three (3) copies of the pre-qualification application shall be submitted – ONE (1) "ORIGINAL", so marked, and TWO (2) endorsed copies each marked "COPY" in separate sealed envelopes. Each envelope shall be clearly marked

IRA/160/2019-2020 EXPRESSION OF INTEREST (EOI) FOR VULNERABILITY ASSESSMENT AND PENETRATION TESTING".

The pre-qualification application must be delivered (by hand or registered mail) to:Tender Box at Insurance Regulatory Authority Offices on 10th Floor, Zep - Re Place, Longonot Road, Upperhill, Nairobi

or be addressed to:

Chief Executive Officer, Insurance Regulatory Authority, 10th Floor Zep Re Place, Longonot Road, Upperhill, P.O. Box 43505 – 00100 Nairobi, Kenya Telephone: +254-20-4996000; 254-719-047000 Email: procurement@ira.go.ke; Website: <http://www.ira.go.ke>

On or before: **18th February 2020 at 10.00hrs**. The EOI shall be opened on **18th February 2020 at 11.00hrs** and in the presence of tenderers' representatives who choose to attend.

Only firms pre-qualified under this procedure will be invited to submit their Technical and Financial proposals under the Request for Proposals (RFP).

CHIEF EXECUTIVE OFFICER/COMMISSIONER OF INSURANCE