SONARWA General

SONARWA General Insurance Company Limited

20th August 2026

REQUEST FOR PROPOSALS (RFP)

To: All Bidders

Dear Sir / Madam,

SONARWA General Insurance Company Ltd has the pleasure to invite all interested companies to submit proposals for **Vulnerability assessment and Penetration Testing Consultancy services**.

The provision of this service should be conducted in an open and transparent manner.

More details on the requirements for this tender are provided in the related Terms of Reference document attached.

The successful Company will be selected under Quality and Cost Based Selection (QCBS) and in accordance with SONARWA General Procurement Policy.

Please submit your proposal not later than 4th September 2026 at 4pm.

ATTN:
1.SONARWA General Insurance Company Ltd
RSSB Tower II
Kigali, Rwanda

For and on hehalf of SONARWA General Insurance Company Ltd

Jean De Dieu Bucyana,

PROCUREMENT MANAGER

SONARWA General Insurance Co. Ltd PROCUREMENT

SONARWA General

TERMS OF REFERENCE (TOR)

Vulnerability Assessment and Penetration Testing (VAPT)

1. Background

SONARWA GENERAL INSURANCE & SONARWA LIFE ASSURANCE seek to strengthen their cybersecurity posture by conducting internal and external vulnerability assessments and penetration testing on critical systems, in line with best practices and compliance requirements.

2. Objectives of the Assignment

- Identify vulnerabilities within internal and external infrastructure.
- Assess the effectiveness of current security controls.
- Attempt to exploit identified vulnerabilities in a controlled manner.
- Provide recommendations for remediation and risk mitigation.
- Support compliance with cybersecurity and data protection standards.

3. Scope of Work

3.1.1 External Penetration Testing

- Public-facing websites and web applications
- Public IP addresses
- Firewalls, VPNs, email gateways, exposed APIs

3.2 Internal Vulnerability Assessment & Penetration Testing

- Internal network infrastructure
- Servers (Windows, Linux)
- Databases, Active Directory
- Network devices (routers, switches, firewalls)

3.3 Web Application Security Testing

Using OWASP Top 10 methodology:

- Authentication & authorization flaws
- SQL Injection, XSS, CSRF
- Session management weaknesses

3.4 Wireless Network Security Testing

- WLAN assessment
- Rogue access point detection
- Encryption strength review

3.5 Cloud Security Assessment

- Configuration review (Azure, AWS, GCP)
- IAM evaluation
- Cloud logging/monitoring review

3.6 Social Engineering

- Phishing simulation
- Employee awareness assessment

3.7 Awareness Training

- Deliver tailored cybersecurity awareness sessions to both staff and management.
- Cover phishing, social engineering, data handling principles, incident reporting, and cyber hygiene practices.
- Provide attendance lists, session materials, and pre/post evaluation tests.

4. Rules of Engagement

Successful bidder must ensure that during the VAPT activity, level of intrusiveness & boundaries of testing are not violated. Roles and responsibilities of bidders would be as follows but not limited to:

1. Attempting to guess passwords using password-cracking tools.
2. Attempting penetration through perceivable network equipment/addressing and other vulnerabilities.
3. Check if any Vulnerability exists in the Servers, Database, Applications, Network and Security devices in scope without disturbing operations.
4. Sniffing Data or information.
5. To check whether there is any vulnerability present in all IT assets in scope.
6. To ascertain the configuration, placement and deployment of IDS is configured for intrusion detection, suspicious activity on host are monitored and reported to server, firewall and IDS logs are generated and scrutinized.
7. Vulnerabilities of unnecessary utilities residing on Application server.
8. Unnecessary ports or services open/ running on the servers.
9. Effectiveness of Tools being used for monitoring systems and network against intrusions and attacks.
10. If any cases of unauthorized access through hacking, denial of service due to technological failure is possible.
11. Any other items relevant in the case of security, to be included in the bid and not to be considered an additional cost.
12. The assessment should include following sections for testing:
    a. DMZ Zone
    b. Remote Access
    c. Network Security Assessment
    d. Network Security Components
    e. VPNs
13. Provide scheduled updates regarding the project.
14. Provide documents / diagrams detailing the project information in a timely manner.

The VAPT should be comprehensive but not limited to following activities:

- **Network Scanning /Surveying:** Vendor shall identify active hosts on a network, for the purpose of simulating attack and also for network security assessment with the help of suitable procedure/ tools including but not limited to:
    a. Examine Name server responses
    b. Review the outer wall of the network
    c. Review tracks from the target organization
    d. Review Information Leaks
- **Port Scanning**: To find the active ports on server port addresses on a host vendor shall perform the following but not limited to:
    a. Error Checking
    b. Enumerate Systems
    c. Enumerating Ports
    d. Verification of Various Protocol Response
    e. Verification of Packet Level Response
- **Port sweep:** To scan multiple hosts for a specific listening port for potential vulnerabilities.
- **System Identification & Trusted System Scanning:** Vendor shall perform the SITS scanning which would include but not limited to the following :-
    a. Match each open port to a service and protocol.
    b. Identify server uptime to latest patch releases.
    c. Identify the application behind the service and the patch level using banners or fingerprinting.
    d. Verify the application to the system and the version.
    e. Locate and identify service remapping or system redirects.
    f. Identify the components of the listening service.
    g. Use UDP-based service and Trojan requests to all the systems in the network.
- **Wireless Leak Tests:** Vendor shall perform the vulnerability assessment & wireless leak test. This may include the following activities:
    a. Verification of the distance in which the wireless communication extends beyond the physical boundaries of the organization.
    b. List equipment needed/tried should be taken (antenna, card, amplifier, etc.)

c. Verification of authentication-method of the clients
d. Verification of that encryption is configured and running - and what key length used
e. Verification of that clients can't be forced to fall-back to plaintext-mode
f. Verification of the IP-range of the network
g. Verification of the IP-range and reachable from the wireless network, and the protocols involved
h. Probe network for possible DoS problems.

- **Vulnerability Scanning**: Vendor shall carry out VA for entire IT assets mentioned in Annexure and addendum if added in future
- **Malware Scanning**: Vendor shall do exhaustive scanning for hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.
- **Spoofing**: Vendor shall assess the scope of potential spoofing attacks i.e, IP, ARP etc and other applicable ones in the Company's environment
- **Security Policy Review:** Vendor shall carry out the review & assessment of Security Policies already in place & Check Point firewalls installed in the Company.
- **Services Probing**: Vendor shall do the following in connection with the following:-
    a. Web Tracks
    b. Mail Tracks
    c. Name Services
    d. Visible Documents
    e. Anti-Virus and Trojan
- **Application Security Testing & Code Review:** In case of some application whose code review is allowed to be done for the purpose of VAPT
- **Access Control Mapping:** ACL has to be reviewed and recommended for improvement.
- **Assessment of OS Hardening:** Vendor shall carry out the the assessment of OS hardening tomcheck & explore the gap in hardening , patch management etc.
- **Denial Of Service (DOS) Attacks:** Following points may be looked for DoS attack:
    a. Verify that administrative accounts and system files and resources are secured properly and
    b. all access is granted with "Least Privilege".
    c. Check the exposure restrictions of systems to non-trusted networks
    d. Verify that baselines are established for normal system activity
    e. Verify what procedures are in place to respond to irregular activity.

f. Verify the response to SIMULATED negative information (propaganda) attacks.
g. Test heavy server and network loads.

- **DDOS Attacks:** All the steps as mentioned for DoS attack has to be verified.
- **Authorization** Testing: Vendor shall do the authorization & authentication testing for the present AD system.
- **Lockout Testing:** To mitigate the brute force attack etc., lockout testing must be carried out.
- **Password Cracking:** To mitigate the brute force attack, cryptographic attack etc., Password cracking testing must be carried out.
- **Cookie Security:** Vendor shall review the cookie settings and recommend the best practise for making the environment secure.
- **Cookie & Web Bug Analysis:** Vendor shall review the cookie for bugs and recommend the best practise for making the environment secure
- **Functional validations:** Any or all application when offered for functional validation, vendor shall perform the same.
- **Containment Measure Testing:** The vendor shall perform this test also wherever applicable.
- **DMZ Network Architecture Review**: Vendor shall review the present DMZ Network Architecture and recommend for the improvement if any.
- **Server Assessment (OS Security Configuration) :** Vendor shall review the present configuration of critical servers and recommend for the improvement if any.
- **Security Device Assessment:** Vendor shall review the present security devices and recommend for the improvement if any.
- **Network Device Assessment:** Vendor shall review the present network devices and recommend for the improvement if any.
- **Database Assessment:** Vendor shall review the present databases and recommend for the improvement if any.
- **Website Assessment (Process):** Vendor would do the assessment of internet facing application as mentioned in the subsequent section with and without credentials having different access levels like operator, supervisor, administrator, etc, to check for vulnerabilities like privilege escalation, input validation, etc.
- **Vulnerability Research & Verification:** Vendor shall conduct the research including but not limited to the following:

a. Integrate the currently popular scanners, latest scanning definitions/signatures, hacking tools, and exploits into the tests.
b. Measure the target Company against the currently popular scanning tools.
c. Attempt to determine vulnerability by system and application type.
d. Attempt to match vulnerabilities to services.
e. Attempt to determine application type and service by vulnerability.
f. Perform redundant testing with at least 2 automated vulnerability scanners.
g. Identify all vulnerabilities according to applications.
h. Identify all vulnerabilities according to operating systems.
i. Identify all vulnerabilities from similar or like systems that may also affect the target systems.
j. Verify all vulnerabilities found during the exploit research phase for false positives and false negatives.
k. Verify all positives.

In addition to the above vendor shall perform Manual Vulnerability Testing and Verification also.

- **IDS/IPS review & Fine tuning of Signatures:** Vendor shall perform the IDS /IPS review including but not limited to the following:
    a. IDS and features identification
    b. Placement of IDS in the network
    c. Testing IDS configuration
    d. Reviewing IDS logs and alerts
- **Man in the Middle attack:** To rule out the possibilities of eavesdropping the MIMA has to be accrued out
- **Man in the browser attack :** To rule out the possibilities of eavesdropping the MIBA has to be accrued out
- **Social Engineering:** The vendor shall carry out social engineering for users at HO, IT staff & ROs.

This may include request testing, guided testing & trusted people testing. This may include the following but not limited to:

a. Select a person or persons from information already gained about personnel

b. Examine the contact methods for the people from the target organisation
c. Invite the people & Gather information from them
d. Enumerate the type and amount of privileged information disclosed.

- **Trusted Systems Testing:** The validity of trusted system also has to be checked.
- **Directory Traversal:** Directory Traversal is a type of HTTP exploit that is used by attackers to gain unauthorized access to restricted directories and files.
- **Keyloggers**: Keyloggers are a form of spyware where computer users are unaware their actions are being tracked.
- **Rootkit:** Vendor would assess the systems to see the presence or probability of presence of rootkit.
- **Botnet:** Vendor would assess the system to see the presence of botnet.
- **Any other attacks & Scenario Analysis:** Apart from all the above-mentioned line item if any activity required of felt by the Company as well as vendor has to be carried out.

Website/Web- Application assessment should be done as per latest OWASP guidelines including but not limited to the following:

- SQL Injection
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Insecure Direct Object References
- Security misconfiguration
- Insecure Cryptographic Storage
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Known Vulnerable Components
- Un-validated Redirects and Forwards
- Failure to Restrict URL Access
- Insufficient Transport Layer Protection
- Any other attacks, which are vulnerable to the web sites and web Applications

The vendor has also to perform the following activities to assess the internet facing applications:

- **Re-Engineering**
    a. Decompose or deconstruct the binary codes, if accessible.

b. Determine the protocol specification of the server/client application.
c. Guess program logic from the error/debug messages in the application outputs and program behaviours/performance.

- **Authentication**
  a. Find possible brute force password guessing access points in the applications.
  b. Find a valid login credentials with password grinding, if possible.
  c. Bypass authentication system with spoofed tokens.
  d. Bypass authentication system using Injection attacks.
  e. Bypass authentication system with replay authentication information.
  f. Determine the application logic to maintain the authentication sessions - number of (consecutive) failure logins allowed, login timeout, etc.
  g. Determine the limitations of access control in the applications - access permissions, login session duration, idle duration.
  h. Determine the transmission of authentication credentials in clear text/ encrypted/ hash form.
- **Session Management**
  a. Determine the session management information - number of concurrent sessions, IP-based authentication, role-based authentication, identity-based authentication, cookie usage, session ID in URL encoding string, session ID in hidden HTML field variables, etc.
  b. Guess the session ID sequence and format
  c. Determine the session ID is maintained with IP address information; check if the same session information can be retried and reused in another machine.
  d. Determine the session management limitations - bandwidth usages, file download/upload limitations, transaction limitations, etc.
  e. Gather excessive information with direct URL, direct instruction, action sequence jumping and/or pages skipping.
  f. Gather sensitive information with Man-In-the-Middle attacks.
  g. Inject excess/bogus information with Session-Hijacking techniques.
  h. Replay gathered information to fool the applications.
- **Input Manipulation**
  a. Verify that input validation is happening at client or server or both end.
  b. Find the limitations of the defined variables and protocol payload - data length, data type, construct format, etc.

c. Use exceptionally long character-strings to find buffer overflows vulnerability in the applications. Concatenate commands in the input strings of the applications.
d. Inject SQL language in the input strings of database-tiered web applications.
e. Examine "Cross-Site Scripting" in the web applications of the system.
f. Examine unauthorized directory/file access with path/directory traversal in the input strings of the applications.
g. Use specific URL-encoded strings and/or Unicode-encoded strings to bypass input validation mechanisms of the applications.
h. Execute remote commands through "Server Side Include".
i. Manipulate the session/persistent cookies to fool or modify the logic in the server-side web applications.
j. Manipulate the (hidden) field variable in the HTML forms to fool or modify the logic in the server-side web applications.
k. Manipulate the "Referrer", "Host", etc. HTTP Protocol variables to fool or modify the logic in the server-side web applications.
l. Use illogical/illegal input to test the application error-handling routines and to find useful debug/error messages from the applications.

- **Output Manipulation**
  a. Retrieve valuable information stored in the cookies
  b. Retrieve valuable information from the client application cache.
  c. Retrieve valuable information stored in the serialized objects.
  d. Retrieve valuable information stored in the temporary files and objects.
  e. Retrieve bulk information/ multiple rows from database.
- **Information Leakage**
  a. Find useful information in hidden field variables of the HTML forms and comments in the HTML documents.
  b. Find valuable information stored in the HTML source code on browser like Unencrypted View State
  c. Examine the information contained in the application banners, usage instructions, welcome messages, farewell messages, application help messages, debug/error messages, etc.

Penetration Testing

To identify ways to exploit vulnerabilities to circumvent or defeat the security features of system components through manual process that may include the use of vulnerability scanning or other automated tools, resulting in a comprehensive report.

- **Black Box Testing**

  Scanning of all critical documents has to be taken up initially. For all the critical applications and data vendor is required to perform Black Box testing and thereby perform the penetration test to simulate an external hacking or cyber warfare attack both at Application layer as well as Network layer. The vendor shall also carry out the segmentation check.

- **White Box Testing**

  With knowledge of the internal structure/design/implementation of the application/object allowed to be tested vendor shall perform the White Box testing both at Application layer as well as Network layer. The vendor shall also carry out the segmentation check.

- **Gray Box Testing**

  Successful vendor shall also perform Gray Box Testing both at Application layer as well as Network layer. The vendor shall also carry out the segmentation check.

5. Methodology

The Consultant shall adopt a structured, industry-recognized methodology to ensure a comprehensive and controlled assessment. The methodology must include, at minimum, the following phases:

5.1 Planning & Preparation

- Conduct a kickoff meeting with the Institution to agree on scope, targets, point of contact, communication protocol, and rules of engagement.
- Define testing windows that minimize business disruption.
- Gather required information such as network diagrams, asset lists, IP ranges, URLs, and user roles for testing.

5.2 Reconnaissance & Information Gathering

- Perform passive and active reconnaissance to understand the Institution's environment.
- Identify publicly available information (OSINT) that may lead to attack vectors.
- Detect exposed services, applications, ports, versions, and potential weak configurations.

5.3 Vulnerability Identification & Analysis

- Conduct authenticated and unauthenticated scanning using industry-grade tools.
- Perform **manual verification** of all findings to eliminate false positives.
- Benchmark vulnerabilities against:
    - CVSS v3.1
    - Known exploits (Exploit-DB, Metasploit, NIST NVD)
    - OWASP Top 10
    - MITRE ATT&CK techniques
- Assess business impact and likelihood in the context of the Institution’s environment.

5.4 Exploitation (Controlled)

- Attempt exploitation of identified vulnerabilities following ethical hacking principles.
- Validate risks by demonstrating controlled exploitation without harming systems.
- Attempt privilege escalation, lateral movement, and access to sensitive resources (within scope).

5.5 Post-Exploitation & Impact Analysis

- Evaluate the extent of compromise possible once a system is breached.
- Highlight business impact such as data exposure, unauthorized access, or system manipulation.
- Document attack paths and risk propagation scenarios.

5.6 Reporting

- Provide clear, evidence-based reporting with screenshots, logs, and step-by-step reproduction.
- Present executive summaries for management and technical details for IT/security teams.
- Prioritize findings by severity and business impact.

5.7 Retesting

- Conduct a full retest after remediation by the Institution.
- Validate closure of previously identified vulnerabilities.
- Deliver a retest report clearly showing:
    - Resolved vulnerabilities
    - Partially resolved findings
    - Unresolved findings and residual risks

6. Deliverables

6.1 Inception Report (Due after 1 week of commencement)

The Consultant shall submit an Inception Report within **7 calendar days** from the commencement date.
The report must include:

- Refined scope and objectives
- Testing methodology and tools
- Detailed work plan and schedule
- Key milestones and deliverables
- Communication and escalation plan
- Access and resource requirements
- Risk management considerations
- Final list of assets and systems to be tested

6.2 Draft VAPT Report

Submitted after completion of all testing activities. Must include:

- Executive summary in non-technical language
- Risk overview and threat landscape
- Detailed technical findings
- CVSS scoring and severity ratings
- Screenshots, evidence, reproduction steps
- Attack paths and exploitation narrative
- Impact analysis per system
- Remediation recommendations with timelines
- Technical appendix containing logs and scripts

6.3 Final VAPT Report & Presentations

Delivered after incorporating feedback on the draft report. Includes:

- executive Summary revised report
- Detailed technical report
- Management PowerPoint presentation
- Technical debrief session with IT/security teams
- Recommendations roadmap (short-term, medium-term, long-term)
- Risk register

6.4 Cybersecurity Awareness Training

The Consultant shall:

- Deliver at least **two structured training sessions**
  - One for management
  - One for general staff
- Provide training materials (slides, handouts, videos if applicable)
- Conduct pre- and post-training assessments
- Submit attendance lists and evaluation results
- Provide a Training Delivery Report

6.5 Retesting Report

- Conduct retesting after the Institution fixes vulnerabilities.
- Validate all findings and update their status.
- Provide a **Retest Report** showing:
  - Closed vulnerabilities
  - Open vulnerabilities
  - Remaining risks and recommendations

The reports must have the following items:

a. **Executive Summary**: Brief high-level summary of the penetration test scope and major findings with overall severity graph.
b. **Statement of Scope:** A detailed definition of the scope of the network and systems tested as part of the engagement, Clarification of Environment vs. non- Environment systems or segments that are considered during the test, Identification of critical systems in or out of the Environment and explanation of why they are included in the test as targets.
a. **Review of past threats & vulnerabilities:** This will include all the threats & vulnerabilities identified and based on those the vendor would carry out the VAPT again.
b. **Statement of Methodology:** Details on the methodologies used to complete the testing (port scanning, nmap etc.)
c. **Limitations:** Document any restrictions imposed on testing such as designated testing hours, bandwidth restrictions, special testing requirements for legacy systems, etc.

d. **Segmentations:** Provide details as to the testing methodology and how testing progressed. For example, if the environment did not have any active services, explain what testing was performed to verify restricted access. Document any issues encountered during testing (e.g., interference was encountered as a result of active protection systems blocking traffic).
e. **Summary of test results:** Detailed results for vulnerabilities discovered, exploited vulnerabilities and proof of concepts/screenshots, detailed explanations of the implications of findings, business impacts, and risks for each of the identified exposures.
f. **Recommendations:** Remediation recommendations to close the deficiencies identified. Detailed steps (wherever/whenever applicable) to be followed while mitigating the reported deficiencies. Security issues that pose an imminent threat to the system are to be reported immediately.
g. **Tools Used:** Details of all the tools used and for the purpose & target system and its impact.
h. **Clean up:** After testing there may be tasks the tester or customer needs to perform to restore the target environment (i.e., update/removal of test accounts or database entries added or modified during testing, uninstall of test tools or other artifacts, restoring active protection-system settings, and/or other activities the tester may not have permissions to perform, etc.). Provide directions on how clean up should be performed and how to verify that security controls have been restored.

7. Duration of Assignment

The entire assignment is expected to be completed within a maximum of **30 calendar days**.

Reporting Structure

The Consultant shall report to:

- The IT Security Personnel
- The Head of ICT
- The Data Protection Officer, for matters involving personal data
- Head of Risk & Compliance
- with copy to Chief Executive Officers of Both Sonarwa GI and Sonarwa Life.

The Consultant must:

- Provide weekly status updates
- Immediately report any critical vulnerabilities posing imminent threat
- Maintain confidentiality and professionalism throughout the engagement

8. SUBMISSION REQUIREMENTS

Administrative documents:

- Trade Licenses/ Company Registration certificate
- Valid Tax Clearance Certificate
- RSSB Clearance Certificate is Registered in Rwanda.
- Cover Letter

Technical Requirements

- **Company Profile** – Detailed profile demonstrating the firm's technical capabilities, years in operation, and history of providing cybersecurity consultancy services.
- **Team Structure & Qualifications** – Provide the organizational structure of the proposed engagement team along with their education, qualifications /certifications in their respectful domain.
- **References**– Certificate of completion for similar work with at least *three corporate institutions*, preferably in Finance/Insurance or other regulated sectors.
- **Project Work Plan** – Clear timeline with milestones (Inception Report, Assessment, Reporting, Awareness Training, Closure).
- **Description of Work** – Clear technical approach for network, system, and application testing.
- **Fees and Compensation** – Detailed and itemized pricing, fixed for the duration of the assignment.
- **Independence & Objectivity** – Declaration of no conflict of interest.

9. Other Points to note

- SONARWA LIFE and SONARWA GI will undertake a due diligence assessment and screening of the preferred Bidder to include reference checks.
- SONARWA LIFE and SONARWA GI 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.
- SONARWA LIFE and SONARWA GI reserve the right to accept any tender (s) or to reject all tenders at any time. SONARWA LIFE and SONARWA GI also reserve 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 regarding this procurement process, please write to **procurement@sonarwa.co.rw** with the subject vulnerability assessment penetration test. SONARWA LIFE and SONARWA GI procurement team will acknowledge receipt of the complaint by email within three (3) working days.

10. CONTACT INFORMATION

- Each bidder shall submit one (1) single document combining both the Technical Offer and the Financial Offer, clearly divided into two distinct sections as follows:

  Part I: Technical Offer

  Part II: Financial Offer

- The document shall be encrypted with a password. The password will be sent via email to: **dpo@sonarwa.co.rw**.

- The encrypted document will be submitted online via email to: **procurement@sonarwa.co.rw.**

- For inquiries, please contact by email: **procurement@sonarwa.co.rw**