REQUEST FOR PROPOSAL (RFP)

Cybersecurity Assessment, Vulnerability Assessment, and Penetration Testing (VAPT)

1. Introduction

Church World Services (CWS) invites qualified and experienced cybersecurity firms to submit proposals for the provision of **Cybersecurity Assessment, Vulnerability Assessment, and Penetration Testing (VAPT)** services.

The purpose of this RFP is to identify a competent Consultant to assess vulnerabilities, evaluate existing security controls, and enhance the organization's cybersecurity resilience.

2. Background

CWS operates in a dynamic and evolving threat landscape requiring continuous evaluation of its information security posture. This engagement aims to proactively identify weaknesses across infrastructure, applications, and networks and to strengthen safeguards against cyber threats.

3. Objective of the Assignment

The selected Consultant will:

- Identify vulnerabilities across systems and infrastructure;
- Evaluate effectiveness of existing security controls;
- Conduct simulated attacks to test defensive capabilities;
- Provide a prioritized remediation roadmap to mitigate risks.

4. Scope of Work

4.1 Information Security Assessment

- Review configurations of firewalls, EDR systems, routers, switches, and Microsoft 365.
- Assess cloud environments (AWS, Azure, GCP) against CIS benchmarks.
- Evaluate security policies and governance practices.

4.2 Vulnerability Assessment

- Identify all in-scope assets and services.
- Perform automated and manual vulnerability scans.
- Assess both internal and external environments.

4.3 Penetration Testing

- Conduct controlled exploitation of identified vulnerabilities.
- Test privilege escalation scenarios.
- Assess lateral movement across systems.
- Perform application and API security testing aligned with OWASP Top 10.

5. Technical Environment (Assets in Scope)

Asset Category	Description
External IPs	Public-facing systems
Internal IPs	Servers, endpoints, IoT
Web Applications	Internal and external portals
Wireless Networks	On-site infrastructure

6. Methodology Requirements

The Consultant must apply industry-standard frameworks, including:

- OWASP;
- OSSTMM;
- NIST SP 800-115.

7. Deliverables

The Consultant shall provide:

- Inception Report (methodology, tools, work plan);
- Immediate alerts for critical vulnerabilities;
- Draft Technical Report (detailed findings and evidence);
- Final Report (executive summary + technical details);
- Remediation Plan with prioritized actions;
- Clean-up confirmation report;
- Re-validation testing report.

8. Duration and Location

- Duration: 12 months
- Location: Nairobi (on-site with remote components where applicable)

9. Vendor Eligibility Criteria

Mandatory Requirements

- Minimum 5 years' experience in cybersecurity consulting;
- Proven experience in VAPT engagements;
- Valid professional indemnity insurance.

Preferred Qualifications

- Certifications such as OSCP, CISSP, or CISM.

10. Proposal Submission Requirements

Proposals must include:

10.1 Technical Proposal

- Company profile and relevant experience
- Proposed methodology and tools
- Work plan and timelines
- Team composition and CVs

10.2 Financial Proposal

- Detailed cost breakdown (professional fees, tools, travel if applicable)
- Pricing structure (fixed, milestone-based, or other)

11. Evaluation Criteria

Proposals will be evaluated using the following criteria:

Criteria	Weight	Description
Relevant Experience	25%	Extent to which the bidder demonstrates experience in similar projects (scope, size, complexity, and industry). Includes demonstrated understanding of client environment and success in comparable assignments.
Technical Approach & Methodology	30%	Quality, clarity, and feasibility of the proposed approach. Includes methodology, work plan, innovation, risk management, timelines, and alignment with project objectives.
Team Qualifications	20%	Competence and suitability of the proposed team. Considers qualifications, certifications, relevant experience, roles/responsibilities, and availability of key personnel.

Cost Effectiveness	15%	Value for money considering total cost vs. expected outcomes. Evaluates pricing transparency, competitiveness, cost breakdown, and alignment with proposed technical solution (not just lowest price).
Past Performance / References	10%	Quality of previous client feedback and evidence of successful delivery. Includes reference checks, track record, reliability, and client satisfaction.

12. Evaluation Process

- **Stage 1:** Compliance check (mandatory requirements)
- **Stage 2:** Technical evaluation
- **Stage 3:** Financial evaluation
- **Stage 4:** Combined scoring and final selection

13. Contract Management and Governance

- Weekly progress meetings will be held;
- Critical vulnerabilities must be escalated immediately;
- A CWS focal point will oversee the engagement.

14. Confidentiality and Ethical Requirements

The Consultant shall:

- Sign a Non-Disclosure Agreement (NDA);
- Ensure minimal disruption to operations;
- Comply with applicable data protection regulations;
- Provide testing source IP addresses in advance;
- Avoid DoS testing unless explicitly authorized.

15. Submission Instructions

- Proposals must be submitted electronically in PDF format
- Submission deadline: **[Insert Date]**
- Submission email:**[Insert Email Address]**
- Subject line:**"RFP – Cybersecurity VAPT Services"**

16. Disclaimer

CWS reserves the right to:

- Accept or reject any proposal in whole or in part;
- Request additional information from bidders;
- Cancel the RFP process at any stage without liability.