BLESSING PHIRI | TECHNICAL SOLUTIONS ENGINEER

Technical Proposal and Statement of Work

Vulnerability Assessment and External Black-Box Penetration Testing

Prepared for: A statutory regulatory board, Southern Africa

Reference	**SAMPLE-PT-001**
Version	**1.1 (sample)**
Status	**Final**
Prepared by	**Blessing Phiri**

Portfolio sample

Based on a real bid. Client identity, people, pricing and commercial terms have been removed or changed. Shared to demonstrate proposal structure and technical scoping.

Document control

Item	Detail
Document title	Technical Proposal and Statement of Work: Vulnerability Assessment and External Black-Box Penetration Testing
Reference	SAMPLE-PT-001
Status	Final
Summary	An independent vulnerability assessment and external black-box penetration test of five public-facing IP addresses and one unauthenticated web application.
Response to	Request for Proposal issued by the client (reference withheld)

Contents

Section
1. Executive summary
2. Our understanding of your requirements
3. Scope of work
4. Technical approach and methodology
5. Rules of engagement and safety controls
6. Deliverables and reporting
7. Risk rating
8. Work plan and effort
9. Client responsibilities and assumptions
10. Delivery team
11. Acceptance and next steps

1. Executive summary

Thank you for the opportunity to respond to your request for an independent vulnerability assessment and external black-box penetration test of five public-facing IP addresses and one unauthenticated web application.

As a regulated statutory board handling sensitive industry, stakeholder and market data, your external attack surface carries both operational and regulatory risk. This proposal sets out a structured, standards-aligned approach that identifies and proves real exploitability from the viewpoint of an unauthenticated outside attacker, while protecting the availability of production services.

The engagement covers:

- Port and service enumeration and external attack-surface mapping
- Testing of one unauthenticated web application and services discovered on the in-scope addresses
- Authentication, encryption, misconfiguration and exposure analysis
- Assessment of firewall, filtering and perimeter-control weaknesses
- Manual validation of findings, CVSS scoring and business-aligned risk ratings
- A technical report, an executive summary and one post-remediation re-test

The outcome is an evidence-based view of your external security posture, a prioritised remediation roadmap, and documented assurance to support your annual third-party security assessment and regulatory obligations.

At a glance	
Targets	5 public-facing IPs and 1 unauthenticated web application
Testing model	External, black-box, fully remote
Total effort	61 hours across three fixed packages
Re-test	1 round included
Standards	OWASP, NIST SP 800-115, ISO/IEC 27001:2022, MITRE ATT&CK;, CVSS

2. Our understanding of your requirements

You require an independent test that validates the effectiveness of your perimeter controls and identifies vulnerabilities, misconfigurations, exposed services, authentication weaknesses, encryption weaknesses and other externally exploitable conditions.

From the RFP, a successful engagement depends on:

- A clearly defined scope, confirmed during a project definition workshop
- Timely access to the in-scope addresses, application details and escalation contacts
- Coordination with the ICT personnel responsible for the in-scope systems
- A structured methodology aligned to internationally recognised standards
- Clear documentation of exploitable weaknesses and control gaps
- Reporting that supports both remediation planning and internal governance

Key requirement: automated scanning alone is not accepted as penetration testing. Every material finding will be manually validated to remove false positives and demonstrate realistic exploitability.

Requested deliverables

No.	Deliverable	Description
1	Kick-off and rules of engagement	Confirmed scope, testing window, source IPs, escalation matrix, safety controls and communication plan, before testing begins.
2	Interim status updates	Progress updates during testing, with immediate notification of critical or high-risk findings.
3	Draft technical report	Findings, affected assets, evidence, CVSS v3/v4 scores, business impact and remediation, within 7 business days of testing.
4	Executive summary report	Non-technical summary of key risks, business impact and remediation roadmap.
5	Final report	Updated report incorporating your review comments.
6	Remediation support	Technical clarification and prioritised remediation guidance.
7	Post-remediation re-test	One re-test and an updated closure and status report.

3. Scope of work

The engagement is a single work stream: a vulnerability assessment and external black-box penetration test of five public-facing IP addresses and one unauthenticated web application hosted on one of those addresses. The addresses will be confirmed after contract award, NDA and approval of the rules of engagement.

In scope

- Port and service enumeration
- External attack-surface mapping
- Testing of the public-facing application and services discovered on in-scope addresses
- Authentication and encryption assessment
- Misconfiguration and exposure analysis
- Firewall, filtering and perimeter-control weaknesses observable externally
- Controlled validation of common external attack vectors using OWASP and NIST practices
- One post-remediation re-test

Out of scope

In line with the RFP, the following are excluded unless separately authorised in writing:

- Internal network penetration testing
- Internal Active Directory testing or lateral movement
- Standalone API or mobile application testing
- Telecommunications core or network-node assessments
- Social engineering by email, telephone or in person
- Denial-of-service, destructive testing or data deletion

4. Technical approach and methodology

We follow a phased methodology that moves from planning to validated, business-rated findings.

Phase	Activities
1. Planning and scoping	Confirm in-scope IPs, rules of engagement, testing windows, source IPs and points of contact.
2. Reconnaissance	Passive and active information gathering to map the external attack surface.
3. Enumeration	Port and service enumeration; weakness identification using automated scanning combined with manual testing.
4. Controlled exploitation	Safely validate vulnerabilities to confirm real-world exploitability without operational risk.
5. Impact analysis	Assess business impact and assign a CVSS-based risk rating to each confirmed finding.
6. Evidence collection	Record sufficient evidence to validate each issue without exposing unnecessary sensitive data.
7. Reporting and close-out	Draft and final technical report, executive summary and management close-out.
8. Re-test	Validate the closure or mitigation of remediated findings.

Standards and frameworks

Framework	How it is applied
OWASP Testing Guide and Top 10	Web application and web-facing service testing
NIST SP 800-115	Overall testing and assessment methodology
ISO/IEC 27001:2022	Mapping findings to relevant security controls
MITRE ATT&CK	Technique mapping for externally exposed systems
CVSS v3 and v4	Consistent, business-aligned severity scoring
Local regulatory expectations	Statutory-body cybersecurity requirements

5. Rules of engagement and safety controls

Testing begins only after written authorisation, NDA execution, scope confirmation and approval of the rules of engagement. The following controls apply throughout:

- Source IP addresses for testing are shared with the client in advance
- Testing windows, escalation contacts, emergency-stop procedures and prohibited techniques are agreed before commencement
- Any critical or high-risk finding that may represent an active threat is reported immediately
- Evidence is minimised, encrypted in transit and at rest, access-controlled and securely disposed of after acceptance
- No credentials, data, screenshots or exploit artefacts are retained beyond the agreed retention period
- Any activity outside the approved scope requires prior written approval

6. Deliverables and reporting

Each finding in the draft and final report contains, at minimum:

Field	Content
Identifier and title	Unique finding ID and descriptive title
Description and assets	What the issue is and which assets are affected
Evidence	Sufficient proof to validate the issue
Attack scenario	Controlled proof of concept or realistic attack path
Risk	CVSS score, likelihood and business impact
Remediation	Clear, actionable recommendation
Re-test status	Closed, partially remediated, risk accepted or open

Report structure

Cover and document control, executive summary, scope and limitations, methodology, findings summary, detailed findings, risk and remediation priorities, re-test results, conclusions and recommendations, appendices.

7. Risk rating

Severity	CVSS range	Expected treatment
Critical	9.0 to 10.0	Immediate escalation and urgent remediation
High	7.0 to 8.9	Prompt remediation, with business impact and priority clearly stated
Medium	4.0 to 6.9	Planned remediation based on risk and exposure
Low	0.1 to 3.9	Addressed through routine security hardening

8. Work plan and effort

Effort is split into three fixed packages so each hour maps to a defined output. Detailed timings are confirmed during the rules-of-engagement workshop.

Package	Description	Deliverable	Hours
PEN-NET-EXT	External black-box test of 5 public-facing IPs	Draft report, executive summary, final report	18
WEB-APP-UN	Black-box test of 1 unauthenticated web application	Web application test report	27
PEN-RETEST	Post-remediation re-test, 1 round	Updated closure and status report	16
		Total	**61**

Factors that may change effort

- Discovery of an active compromise or live incident during testing
- A materially different number of live services than anticipated
- Delays in confirming source IPs, escalation contacts or testing windows

Additional re-testing or scope changes are handled through change control on a time-and-materials basis.

9. Client responsibilities and assumptions

At least two weeks before testing, the client will provide:

- The five in-scope IP addresses and the web application details
- Escalation contacts, agreed testing windows and any prohibited techniques
- An executed NDA and approved rules of engagement
- A technical point of contact able to act on critical findings during testing
- Confirmation of each finding's status ahead of the re-test

This is a fully remote engagement. No on-site presence is required, and findings reflect a point-in-time assessment based on the access and information provided.

10. Delivery team

Role	Responsibility
Lead security consultant	Testing methodology, exploitation and reporting
Senior security consultants	Quality assurance, evidence handling and report review
Technical solutions engineer (in-country)	Client coordination, delivery support and hands-on remediation guidance
Engagement lead	Scope, governance and executive communication

All consultants hold relevant industry certifications and are background-checked.

11. Acceptance and next steps

- Confirm acceptance of this proposal and the commercial quote
- Execute the NDA and approve the rules of engagement
- Hold the kick-off and project definition workshop
- Begin testing in the agreed window

About this sample. This document reproduces the structure and technical content of a real bid response. The client, team members, pricing, legal terms and contact details have been removed or changed. Prepared by Blessing Phiri as a portfolio sample.