Transport Education Training Authority *Driven by Vision*	**TERMS OF REFERENCE**
PURPOSE:	**APPOINTMENT OF A SERVICE PROVIDER TO CONDUCT A PENETRATION TEST TO TETA'S IT INFRASTRUCTURE**

1. THE BACKGROUND AN CONTEXT

The Transport Education and Training Authority (TETA) conducts annual vulnerability assessments and penetration testing as part of its cybersecurity governance and risk management practices. These initiatives aim to strengthen the organization's security posture, ensure alignment with recognized industry standards, and proactively identify and mitigate cyber risks.

The most recent vulnerability assessment was completed during the fourth quarter of the 2024/2025 financial year. As TETA is now in the fourth quarter of the 2025/2026 financial year, a penetration test is due in line with the organization's cybersecurity program. While vulnerability scanning identifies technical weaknesses, it does not validate exploitability or real-world attack scenarios. Penetration testing is therefore required to simulate realistic threat actor techniques, validate remediation effectiveness, and assess the resilience of people, processes, and technology across TETA's environment.

TETA operates across five (5) offices, with the Head Office located in Randburg and regional offices situated in Cape Town, Durban, Limpopo, and Nelspruit. The penetration testing exercise must comprehensively cover all office locations, including their respective network infrastructure, systems, and users.

The scope must further include all web applications and critical business systems used by TETA, including but not limited to:

- Financial Management system
- Learning management system (LMS)
- Payroll system
- Document management system
- Any other internally or externally accessible business applications

1.1. PURPOSE

The purpose of this engagement is to conduct a comprehensive penetration test to:

- Validate the effectiveness of remediation actions taken.
- Identify real-world attack paths and exploitable weaknesses.
- Assess the effectiveness of existing security controls.
- Reduce the risk of data breaches, system compromise, and service disruptions.
- Support compliance with governance frameworks and regulatory requirements.
- Strengthen TETA's cybersecurity maturity.

1.2. OBJECTIVES

The objectives of this engagement are to:

- Simulate real-world cyberattack scenarios.
- Validate whether remediated vulnerabilities remain exploitable.
- Identify weaknesses that could lead to unauthorized access, privilege escalation, or lateral movement.
- Assess the effectiveness of perimeter, internal, and identity-based security controls.
- Provide actionable remediation recommendations.

1.3. SCOPE OF WORK

a. External Environment Testing
   - Assess internet-facing systems, applications, and infrastructure.
   - Identify vulnerabilities, misconfigurations, and exposed services.
   - **Estimated number of external IPs = <5**

b. Internal Environment Testing
   - Evaluate internal network segmentation and trust boundaries.
   - Test endpoint security, privilege escalation, and lateral movement.
   - **Estimated number of internal hosts/endpoints = >300**
   - Number of web apps in scope= 5
   - Cloud tenants and major workloads = 1

c. Identity and Access Management Testing
   - Assess Active Directory and authentication controls.
   - Review privileged account management and access controls.

d. Walkthrough and Validation of Remediation Actions
   - Review remediation actions taken from the recent vulnerability assessment
   - Validate patching, configuration hardening, and updates.
   - Identify residual risks and gaps.

e. Reporting and Recommendations
   - Provide a detailed technical report with findings and risk ratings
   - Deliver an executive summary report.
   - Present prioritized remediation recommendations.

1.4. DELIVERABLES

1.4.1. The service provider shall deliver:

- Penetration Testing Plan and Methodology
- Detailed Technical Report
- Executive Management Summary
- Remediation Validation Summary
- Close-out Presentation

1.4.2. Methodology and Standards

- Testing must align with industry standards including:
- NIST SP 800-115
- OWASP Testing Guide
- PTES
- ISO/IEC 27001

1.4.3. Roles and Responsibilities

Service Provider:

- Conduct penetration testing in accordance with approved scope.
- Ensure confidentiality and non-disruptive testing.
- Deliver accurate and actionable reporting.

TETA:

- Provide access and approvals.
- Facilitate stakeholder engagement.
- Review deliverables and coordinate remediation.

1.5. PROJECT METHODOLOGY AND APPROACH

Provide a detailed project plan (GANTT chart) that response to the project and it must demonstrate the following key areas of consideration:

Planning

a. Kick-off Meeting: Conduct a project initiation meeting between TETA and the service provider to discuss objectives, expectations, and timelines.
b. Asset Identification: Identification and cataloguing of all network assets, including hardware, software, and external IP addresses.
c. Scope Definition: Define the assessment boundaries, target systems, network zones, and business-critical assets.
d. Compliance and Legal Considerations: Ensure compliance with applicable regulations, standards, and internal policies. Confirm appropriate legal authorizations for scanning all parts of the network.
e. Project Plan : **Must demonstrate the following key areas of consideration**
    - Project Phases (based on delivery timelines).
    - Project Activities as outlined above.
    - Timelines.
    - Resource Allocations.

1.6. REPORTING AND DELIVERABLES

Upon completion of the assessment, the service provider must deliver the following reports:

1.6.1. Executive Summary Report

a. Non-technical overview of the findings suitable for management.
b. Key risks and vulnerabilities, potential impacts, and overall security posture of TETA's IT infrastructure.

1.6.2. Technical Detailed Report

a. Comprehensive details on each identified vulnerability, including:
    i. Description and location of the vulnerability.
    ii. The potential impact of exploitation.
    iii. Evidence such as screenshots, logs, or exploit results.
b. Categorization of vulnerabilities by severity (Critical, High, Medium, Low).
c. Recommendations for remediation for each identified vulnerability.

1.6.3. Risk Matrix and Prioritization

a. A risk matrix that categorizes vulnerabilities based on their impact and likelihood of exploitation.
b. Prioritization of remediation efforts based on risk to TETA's operations.

1.6.4. Recommendations

a. Actionable recommendations to mitigate vulnerabilities.
b. Suggested improvements to security configurations, policies, and monitoring practices.
c. Long-term strategies for maintaining network security, including future scans and vulnerability management.

1.7. Security and Confidentiality

The service provider must sign a commitment and adhere to the following:

- **Confidentiality Agreement**:

The service provider must sign a confidentiality and non-disclosure agreement to ensure the security of TETA's sensitive data.

- **Data Handling**:

All collected data must be handled with strict confidentiality, and secure mechanisms should be employed for data transfer and storage.

1.8. Additional - Technical Details of IT Network Elements to Be Assessed

External Network Elements

a. **Public-Facing Servers and Web Applications**
   Web servers, application servers, customer-facing portals, email servers, DNS servers, FTP servers.
b. **Firewall and Perimeter Security Devices**
   Firewalls, VPN gateways.
c. **Cloud-Based Services and Workloads**
   Public cloud services (IaaS, PaaS, SaaS), web hosting, external databases.
d. **External IP Addresses and DNS Configurations**

Internal Network Elements

a. **Servers**
   File servers, database servers, application servers, domain controllers.
b. **Workstations and Endpoints**
   Employee desktops, laptops, mobile devices, printers.
c. **Active Directory (AD) and Identity Management Systems.**
d. **Network Devices**
   Switches, routers, wireless access points (WAPs), and network controllers.
e. **Wireless Networks**
   Corporate Wi-Fi, guest Wi-Fi networks, IoT devices connected to wireless networks.

1.9. Application Security

a. **Custom or Off-the-Shelf Applications**
   Custom-built internal applications, Customer Relationship Management (CRM) Systems, Learning Management Systems (LMS), Enterprise Resource Planning (ERP) systems.
b. **Databases: SQL databases, NoSQL databases, cloud-hosted databases.**

1.10. Workloads and Virtualization Environments

a. Virtual Machines (VMs) and Hypervisors
b. Containerized Applications Docker, Kubernetes workloads.
c. Backup and Recovery Systems

1.11. DELIVERABLES AND EXPECTATIONS

The service provider must deliver the following:

A detailed report on the findings of the assignment for the scope as covered under Section 4: Scope of Work of this terms of reference.
This should include:

a. A detailed penetration Test and presentation on all discovered vulnerabilities.
b. Ratings of identified Vulnerabilities in terms of likelihood and impact.
c. Provide the vulnerability raw data to TETA.
d. Report on any critical risk vulnerabilities that may be identified.
e. Report with recommendations on Remedial Actions for all identified vulnerabilities.

1.12. PROJECT CLOSEOUT REPORT

Executive Summary presentation will be required at the end of the project.
The report must include:

i. key findings from the risk assessment and lead a conclusive discussion on the cybersecurity audit report.
ii. Summary of vulnerabilities that may have been identified during vulnerability assessments with clear dashboard and recommendations
iii. Further recommendations on future work.

1.13. Training and Skills Transfer

The bidder's proposal must outline skills transfer plan that articulates how knowledge and skills will be transferred to TETA ICT Team to build capacity. The training / skills transfer plan outlines the following aspects:
Objectives and goals of the skills transfer plan.
-Nature and scope of the knowledge and skills to be transferred (e.g. Vulnerability Management, Cyber security awareness Campagne.)

2. EVALUATION CRITERIA

This bid will be evaluated in three (3) stages as follows:

Stage 1 - Pre-Compliance (Administrative Compliance) Evaluation
Administrative Requirements
Mandatory Requirements
Stage 2 - Quality / Technical Proposal Evaluation
Stage 3 - Price and Specific Goals Evaluation

2.1 PRE-COMPLIANCE EVALUATION - (STAGE 1)

After the receipt of bids, Supply Chain Management Unit will conduct administrative compliance of bid submissions based on the following mandatory and administrative requirements:

2.2 MANDATORY REQUIREMENTS

Bidders who fail to meet the following mandatory requirements will be disqualified at Pre- Compliance Phase:

Criterion	Requirement
Pricing / Costing Schedule	• Submit the Pricing Proposal / Costing Schedule Electronic submission via email to supply Chain Department.
Declaration of Interest (SBD 4)	• The bidder must fully complete and sign the Declaration of interest form electronically or in black ink. For JV or consortium both parties must complete and sign this declaration, per company.
SARS Pin / CSD Supplier Number	• The bidder must submit a SARS Pin with expiry date to assist with verification of Tax Affairs. • If SARS Pin is not submitted provide CSD Supplier Number. In a case of a JV, both companies' Tax Clearance Certificates or SARS pins must be submitted.
Central Supplier Database **Registration**	• The bidder must be registered as a supplier with Treasury on www.csd.gov.za. (Please attach proof)
Proof of Pen Test Engineer Accreditation	• The bidder must provide certification of engineers in cybersecurity e.g. **(or Similar)** • **E.g. CEH-** Certified Ethical Hacker (widely recognized for procurement) • **CPENT-** Certified Penetration Testing Professional • **CompTIA Pen Test+** • **CPTE -** Certified Penetration Testing Engineer
Track record and References	• The service provider must provide Reference Letter/s demonstrating services rendered in Cybersecurity services e.g. **vulnerability assessment and penetration testing.** Projects were satisfactory delivered from contactable existing/recent clients within the past **Five (5) years.** • Letters must be on the company letterhead and must be dated and signed. The letters must state the start and end date of the project. **No appointment letters / SLA agreements from clients will be accepted as reference letters**

Company Experience	• Service providers should have a minimum of three projects completed in the provision of cybersecurity services (**Vulnerability assessment or Penetration testing**). The experience will be evaluated from the letters provided and a completed experience schedule. **NB**. Complete the respective schedule of the Request for Bid (RFB) and support the listed projects with reference letters.
Project plan	• The service provider must submit a detailed project plan on how the project will be delivered

2.1.1. **Administrative Requirements**

As part of the administrative compliance evaluation, the bidder must also furnish the following documents:

Criterion	**Requirement**
Unsigned bid documents	• For any unsigned documents, bidders will be given 48 hours to submit signed documents.
B-BBEE Certificate	• Preference Points Schedule (B-BBEE) form SBD 6.1 must be completed and signed. • A certified copy of the B-BBEE Certificate must be submitted (not a certified copy of a copy). • Submit a valid BBBEE Verification Certificate from SANAS Accredited Verification Agency / Registered Auditor approved by IRBA. The Qualifying Small Enterprise (QSE) and Exempted Micro Enterprises (EME) must submit an affidavit stamped and signed by the Commissioner of Oath confirming the Company Annual Total Revenue and level of black ownership. • Failure to submit a valid B-BBEE Certificate will result in a bidder losing preference points. • In a case of a JV, a combined B-BBEE Certificate must be submitted together with a JV

	Agreement signed by both parties.
CIPC Documents	• The bidder must provide certified copies of Company / Close corporation registration certificates issued by CIPC. • Bidders must confirm their company registration with CIPC as TETA will not award any tender to any business that appears on the CIPC List of • de-registered businesses.
Identity Documents of Directors/Owners or List of Directors	• Certified copies of Directors/Owners Identity Documents OR • List of directors • **NB.** Documents are needed to claim for Specific Goals.
Company Profile including HDI status	• The bidder is required to provide company background information materials / Company Profile
General Conditions of Contract/Bid	• The bidder must accept General Conditions of • Contract / Bid and provide full and accurate answers posed in this section.
Letter of Authority of Signatory	• The bidder is required to provide a Letter of Authority of Signatory to sign the bid submission, signed and in the company's Letter Head.
Submission of Employment Equity (EE) Compliance Certificate	• The Service Provider must submit Employment Equity Act (EEA) Compliance Certificate or a Declaration as conclusive evidence that the service provider meets the requirements of Chapter 2 (all employers) or Chapter 2 and 3 of the EEA (designated employers)

3. QUALITY EVALUATION – (STAGE 2)

TETA applies the provisions of the **Preferential Procurement Policy Framework Act**, (Act no. 5 of 2000) and the **Preferential Procurement Policy Framework Act Regulations of 2022.**

NB. The following values with their meanings will be applied for evaluation purposes:

Values: 1 = Poor 2 = Average 3 = Good 4 = Very Good 5 = Excellent

The scores will be allocated according to the following **EVALUATION MATRIX** for assessment of bids:

<table>
<tr><th>No.</th><th>QUALITY EVALUATION</th><th>Weighting</th></tr>
<tr><td>3.1 Company experience</td><td>
EXPERIENCE IN THE PROVISION OF CYBERSECURITY SERVICES (VULNERABILITY ASSESSMENT, PENETRATION TESTING) (60) POINTS

Service providers should have a minimum of three projects completed in the provision of cybersecurity services (Vulnerability assessment or Penetration testing).

NB. This experience will be validated against the references furnished below

NB. The bidder must complete the respective Company Experience Schedule, and this information must correspond with the information on the reference letters in order to be allocated points

Where there are discrepancies between the information on Company Experience Schedule and reference letters, TETA reserves the right to award no points to a bidder.

PROJECTS COMPLETED IN THE PROVISIONING OF CYBERSECURITY SERVICES (VULNERABILITY ASSESSMENT, PENETRATION TESTING)
<table>
<tr><td>5 Projects and more</td><td>Excellent (5)</td></tr>
<tr><td>4 Projects</td><td>Very Good (4)</td></tr>
<tr><td>3 Projects</td><td>Good (3)</td></tr>
<tr><td>Less than 3 Projects</td><td>Poor (0)</td></tr>
</table>
</td><td>60</td></tr>
</table>

3.2. Methodology	**METHODOLOGY & PROJECT APPROACH: (40 points)** The bidder must demonstrate an understanding and ability to rollout the project with the following key aspects and time frames (but not limited to): a) Detailed description of the penetration testing and cybersecurity services offered by the bidder. b) A detailed project plan outlining all phases of the engagement, including planning, reconnaissance, vulnerability identification, exploitation, validation, reporting, and remediation verification c) Proposed turnaround times for the completion of testing activities, submission of draft and final reports, and validation testing. d) A detailed skills transfer plan outlining how knowledge will be transferred to the client's internal teams during and after the engagement.		**40**
	Methodology is detailed and includes all of the elements mentioned above	**Excellent (5)**	
	Methodology includes three of the elements mentioned above	**Very Good (4)**	
	Methodology does not include any of the outlined elements mentioned above	**Poor (0)**	
	TOTAL		**100**

NB: Bidders that score less than 70 points out of 100 points on Quality Evaluation will not be evaluated further on Price and Specific Goals Evaluation.

4. PRICE AND SPECIFIC GOALS EVALUATION CRITERIA (STAGE 3)

4.1. Price Evaluation

TETA applies the provisions of the **Preferential Procurement Policy Framework Act, (Act no.5 of 2000) and** the **Preferential Procurement Policy Framework Act Regulations of 2022.**

Preferential points will be allocated using 80/20 as follows: Criteria	**Points**
Price	80
Specific Goals	
B-BBEE status of level contributor	10

Other Specific Goals	10
Total	**100**

$$Ps = 80\left(1 - \frac{Pt - P\min}{P\min}\right)$$

Where

Ps = Points scored for price of tender under consideration

Pt = Rand value of tender under consideration

Pmin = Price of lowest acceptable tender

4.2. Specific Goals Evaluation

The following Table will be used to allocate the scores as this is an 80/20 bid:

B-BBEE Status Level of Contributor	**Number of Points (80/20)**
1	10
2	9
3	7
4	6
5	4
6	3
7	2
8	1
Non-compliant contributor	0
Other Specific Goals	**10**
1. Who had no franchise in national elections before 1983 and 1993 Constitutions	3
2. Who is a female	3
3. Who has disability	2
4. Who is young (youth)	2

NB: The bid will be awarded to a bidder who scores the total highest points on Price and B-BBEE unless there is a compelling reason not to award the bid to the highest point scorer.

5. MONITORING PROGRESS OF ASSIGNMENTS

TETA shall monitor and evaluate the progress of the project through deliverables on an ongoing basis.

6. DURATION OF THE PROJECT

The project must be completed within 21 days(Three weeks) from the day of appointment.

7. APPROVAL

RECOMMENDATION BY THE USER DEPARTMENT					
Recommended [x]		Not recommended [ ]			
Executive Corporate Services	Ms Kgatile Nkala	**Signature:**		**Date:**	18/05/2026

APPROVAL BY SCM					
Recommended [X]		Not recommended [ ]			
SCM Manager	Mr Z. Mangaliso	**Signature:**		**Date:**	17/06/2026

SCHEDULE OF COMPANY'S EXPERIENCE: LIST OF REFERENCES

COMPANY'S NAME:_____

No.	Name of Institution	Project Description (Name of ERP / MIS)	Project Start Date (dd/mm/yyyy)	Project End Date (dd/mm/yyyy)	Name of Reference	Contacts Details of Reference	
						Telephone No.	Email Address
1							
2							
3							
4							
5							
6							

ANNEXURE C: SCHEDULE OF EXPERIENCE OF TECHNICAL PERSONNEL / SECURITY PERSONNEL LIST OF REFERENCES

TECHNICAL PERSONNEL / SECURITY PERSONNEL NAME: _____

No.	Name of Institution	Project Description	Project Start Date (dd/mm/yyyy)	Project End Date (dd/mm/yyyy)	Name of Reference	Contacts Details of Reference	
						Telephone No.	Email Address
1							
2							
3							
4							