

TERMS OF REFERENCE FOR

SOURCING INTERNAL AUDIT SERVICES TO CONDUCT A CYBER SECURITY

AUDIT FOR THE PUBLIC SERVICE SECTOR EDUCATION AND TRAINING

AUTHORITY (PSETA) IN LINE WITH THE APPROVED 2025/2026 INTERNAL

AUDIT PLAN.

RFP/2021/001347

CLOSING DATE: 06 FEBRUARY 2026

CLOSING TIME: 11:00 AM

1. PURPOSE

To provide service providers with the necessary background and information to submit a detailed proposal for conducting the following audit review in quarter 4 of 2025/2026:

- **Cybersecurity Audit Review**

PSETA wants to obtain a comprehensive response (clear and unambiguous) from bidders in terms of their ability to support the delivery of the relevant services.

2. BACKGROUND

PSETA is established in terms of section 9(1) and (2) of the Skills Development Act (Act No. 97 of 1998 as amended). The Skills Development Act is PSETA's enabling legislation and guides its operations as a sector education and training authority (SETA), as set out in section 10 of the Act.

For accountability purposes, the PSETA is a schedule 3A entity of the Public Management Finance Act (PFMA), with its own Accounting Authority which is accountable to the Minister of Higher Education, Science and Innovation. High level structuring of the entity consists of the following programmes:

- Programme 1: Administration
- Programme 2: Skills Planning and Research
- Programme 3: Learning Programmes and Projects
- Programme 4: Quality Assurance

3. RATIONALE FOR THE CYBERSECURITY AUDIT REVIEW.

3.1 PSETA Internal Audit comprises of a CAE and two (02) in-house internal audit staff members. To augment its capacity, a panel of service providers has been established.

3.2 The approved 2025/2026 Internal Audit Plan has, as part of its quarter 4 deliverables, **a Cybersecurity Audit Review**. The internal audit unit does not have in-house ICT audit expertise, hence the need for sourcing the required expertise through the established panel of service provider.

4. OBJECTIVES OF THE CYBERSECURITY REVIEW

PSETA internal audit is seeking to fulfil the following audit objective:

- 4.1** Assurance on the design of policies, systems and technologies in place to protect PSETA's ICT environment from cyber threats.

5. SCOPE OF WORK

The following scope of work applies for the Cybersecurity audit project:

- i. **Review of IT Security Policies and Procedures' compliance with applicable laws, regulations, and industry standards.**
- ii. **Review of IT security policy and security configuration standards for all infrastructure components**
- iii. **A review of IT Security Architecture.**
- iv. **Penetration Testing (Internal and External)**
- v. **Follow-up on 2024/2025 Cybersecurity Audit Report Findings**

6. TIME FRAME

The audit review is planned to commence quarter 4 of 2025/2026, **from 12 February 2026 and be completed by 21 March 2026, latest.** As such, the allocation of capacity should consider the completion timelines as indicated.

7. KEY DELIVERABLES

7.1. PROJECT DELIVERABLES

Deliverable	Explanation	Sign Off
Audit Planning Phase		
1. Project Kick-off	Opening / Audit Entrance Meeting	PSETA Internal Audit Team

Deliverable	Explanation	Sign Off
2. Completed Declaration Forms	Declaration forms are completed prior commencement of actual audit work	PSETA Internal Audit Team
3. Audit Planning Memorandum	Development of an APM map timelines of audit process	PSETA Internal Audit Team
4. Engagement Letter	Drafting of engagement letter to issue to audit client	PSETA Internal Audit Team
5. System Description	Documenting system description	PSETA Internal Audit Team
6. Audit Programme	Assess Risks and Controls; Development of Audit Procedures for testing controls (Audit Programme)	PSETA Internal Audit Team
7. Request for Information (RFI)	Prepare and issue and RFI for approved Audit Programme.	PSETA Internal Audit Team
Execution Phase		
8. Execution of Audit Programme – completed audit working papers	Execute approved Audit Programme and complete relevant working papers	PSETA Internal Audit Team
9. Informal Queries / Draft Findings	Draft informal queries as the audit progresses and discuss with management.	PSETA Internal Audit Team
Reporting		
10. Draft Internal Audit Reports	Draft internal audit report compiled and discussed with management.	PSETA Internal Audit Team
11. Final Internal Audit Reports	Final internal audit report compiled and presented to management.	PSETA Internal Audit Team

Deliverable	Explanation	Sign Off
12. Project Close Out	Quality Assured Audit File	PSETA Internal Audit Team
13. Audit Committee Reporting	Presentation of Internal Audit Report to the Audit Committee.	PSETA Internal Audit Team

8. COMPETENCIES OF PROSPECTIVE SERVICE PROVIDER

8.1. To effectively attend to the audit scope in 5 above, the service provider must provide a multidisciplinary project team, with experience in conducting ICT Security related assurance engagements or services and the following certifications:

- i. Certified Ethical Hacker (CEH)**
- ii. Certified Information Systems Security Professional (CISSP)**
- iii. Certified Cloud Security Professional (CCSP)**
- iv. Certified Information Security Manager (CISM)**
- v. Certified Information Systems Auditor (CISA).**

9. ADMINISTRATION

The service provider must be a registered entity or consortium of companies, with traceable credential and should be able to assume duties immediately on appointment.

10. REPORTING REQUIREMENTS

- 10.1. The appointed service provider shall be required to report to the Chief Audit Executive of the PSETA
- 10.2. All work must be carried and reports finalised line with the Internal Audit methodology and approved working paper templates.
- 10.3. Payment will only take place after the requirements for specific deliverables have been met.

11. SUBMISSION OF THE PROPOSAL

The service provider should prepare an offer/proposal on how the assignment will be undertaken, a clear work plan, and curriculum vitae of the expert(s) as well as reference letters to support experience. The proposal must be concise and straight to the point.

12. RETENTION OF RECORDS

All the information derived and produced during the implementation, licensing, training as well as maintenance and support of the data analytics solution will remain the property of the PSETA.

13. PROPOSAL EVALUATION AND APPOINTMENT OF SERVICE PROVIDER

The proposals will be evaluated on the 80/20 principle with 80 points being allocated for price and 20 points allocated for specific goals once the minimum functionality criteria are met. The evaluation will be based on:

The evaluation will be based on

		Points
Price		80
Special goals		20
Black owned company Bidder who has 51% to 100% black people ownership	8	
Women Bidder who has 51% to 100% women ownership	4	
Youth Bidder who has 51% to 100% youth ownership	5	
Disability Bidder who has 51% to 100% disability ownership	3	
Total		100

14. FORMAT OF THE BID SUBMISSION

13.1 Proposals must be submitted electronically.

13.2 Submission of all applicable documents as indicated below:

- Certified copy of doctor's certification with medical practice number.
- Certified copies of the director's ID's document (in order claim points for disability as per SBD 6.1)
- Certified copy of BB-BEE certificate or sworn affidavit.
- Valid Tax compliance status (TCS) PIN or proof of exemption from SARS.
- Copy of the registration document of the organisation (CIPC).
- Copy of the Central Supplier Database registration.

15. IMPORTANT MANDATORY INFORMATION FOR BIDDERS

15.1. All Standard Bidding documents (SBD) documents must be completed and signed.

- SBD 1 (All sections must be fully completed)
- SBD 4 (All sections must be fully completed)
- SBD 6.1 (All sections must be fully completed)
- Proof of registration on Central Supplier Database.
- General Conditions of Contract (All pages must be signed or initialled)

15.2. To effectively attend to the audit scope in 5 above, the service provider must provide a multidisciplinary ICT Audit related project team, with at least 3 of the following certifications collectively (kindly supply certified copies):

- i. Certified Ethical Hacker (CEH)
- ii. Certified Information Systems Security Professional (CISSP)
- iii. Certified Cloud Security Professional (CCSP)
- iv. Certified Information Security Manager (CISM)
- v. Certified Information Systems Auditor (CISA).

NB: Please note that failure to submit documents requested on section 15 will render the proposal disqualified.

Submissions must be sent electronically to KhutsoM@pseta.org.za