Woodpecker Building | Hillcrest Office Park
177 Dyer Rd | Hatfield | Pretoria | 0083
Tel: +27 12 423 5700 | **Fax:** +27 12 423 5755/65
communications@pseta.org.za | www.pseta.org.za

TERMS OF REFERENCE FOR

SOURCING INTERNAL AUDIT SERVICES TO CONDUCT A CYBERSECURITY REVIEW FOR THE PUBLIC SERVICE SECTOR EDUCATION AND TRAINING AUTHORITY (PSETA) IN LINE WITH THE APPROVED 2026/2027 INTERNAL AUDIT PLAN'S QUARTER 4 DELIVERABLES.

RFP/2021/

CLOSING DATE: 13 NOVEMBER 2026

CLOSING TIME: 11:00

1. PURPOSE

To provide service providers with the necessary background and information to submit a detailed proposal for conducting the following review in **quarter 4 of 2026/2027**:

- **Cybersecurity Review *(Ref. 2026/27- 20)***

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 REVIEW.

3.1 PSETA Internal Audit comprises of a CAE and two (02) in-house internal audit staff members. To augment its capacity, the CAE has embarked on sourcing service providers to assist with the implementation of specific internal audit projects, as approved by the Audit Committee.

3.2 The approved 2026/2027 Internal Audit Plan has, as part of its **quarter 4 deliverables,** planned assurance project on Cybersecurity.

4. OBJECTIVES OF THE CYBERSECURITY REVIEW

PSETA internal audit is seeking a service provider to provide internal audit review to fulfil the following audit objectives:

4.1 Cybersecurity Review - 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 audit scope of applies for the audit project:

5.1 Review of IT Security Policies and Procedures' compliance with applicable laws, regulations, and industry standards.

5.2 Review of IT security policy and security configuration standards for all infrastructure components.

5.3 A review of IT Security Architecture; and

5.4 Penetration Testing (Internal and External)

6. TIME FRAME

The audit review is planned to commence **quarter 4 of 2026/2027**, from **18 January 2027 and be completed by 26 February 2027,** latest. As such, the allocation of capacity should consider the completion timelines as indicated.

7. KEY DELIVERABLES

7.1. PROJECT DELIVERABLES

Deliverable	Explanation	Responsibility / Sign Off
Audit Planning Phase		
1. Project Kick-off	Opening / Audit Entrance Meeting	CAE and co-sourced service provider
2. Completed Declaration Forms	Declaration forms are completed prior commencement of actual audit work	Co-sourced service provider

Deliverable	Explanation	Responsibility / Sign Off
3. Audit Planning Memorandum	Development of an APM map timelines of audit process	Co-sourced service provider, signed off by CAE
4. Engagement Letter	Drafting of engagement letter to issue to audit client	Co-sourced service provider, signed off by CAE
5. System Description	Documenting system description	Co-sourced service provider – ensure signoff by audit client.
6. Audit Programme	Development of Audit Procedures for testing controls (Audit Programme)	Co-sourced service provider, signed off by CAE
7. Request for Information (RFI)	Prepare and issue and RFI for approved Audit Programme.	Co-sourced service provider
Execution Phase		
8. Execution of Audit Programme – completed audit working papers	Execute approved Audit Programme and complete relevant working papers	Co-sourced service provider
9. Informal Queries / Draft Findings	Draft informal queries as the audit progresses and discuss with management.	Co-sourced service provider
Reporting		
10. Draft Internal Audit Report	Draft internal audit report compiled and discussed with management.	Co-sourced service provider
11. Final Internal Audit Reports	Final draft internal audit report presented to CEO.	Co-sourced service provider and CAE
	Final report signed by co-signed by co-source provider and forwarded to CAE	Co-sourced service provider

Deliverable	Explanation	Responsibility / Sign Off
12. Client Satisfaction Survey	Issue of Client Satisfaction Survey form to audit client	Co-sourced service provider
13. Project Close Out	Quality Assured Audit File – **05 March 2027**	Co-sourced service provider
14. Audit Committee Reporting	Presentation of Internal Audit Report to the Audit Committee – on request.	Co-sourced service provider

8. COMPETENCIES OF PROSPECTIVE SERVICE PROVIDER

The prospective service provider MUST satisfy required competencies as listed on the functionality criteria in 13 below to be considered.

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 specified 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 functionality criteria (phase 1) and 80/20 principle (phase 2) with 80 points being allocated for price and 20 points allocated for specific goals once the minimum functionality criteria are met.

PHASE 1: FUNCTIONALITY EVALUATION

Bids must meet the minimum eligibility criteria in respect of functionality of **70 points out of 100 points** that will be awarded for functionality before they are considered further. Any bid that does not meet the minimum eligibility threshold will be automatically disqualified.

Below are the applicable functionality criteria for the bid:

Woodpecker Building | Hillcrest Office Park
177 Dyer Rd | Hatfield | Pretoria | 0083
Tel: +27 12 423 5700 | **Fax:** +27 12 423 5755/65
communications@pseta.org.za | www.pseta.org.za

DOMAIN	EVALUATION METHOD	CRITERIA	WEIGHT
1. Professional Certifications	1.1 The service provider must provide a multidisciplinary project team, which collectively possess the following certifications: • Certified Internal Auditor (CIA) • Certified Information Systems Auditor (CISA) • Certified Ethical Hacker (CEH) • Certified Information Systems Security Professional (CISSP) • Certified Cloud Security Professional (CCSP) • Certified Information Security Manager (CISM) **NB: Certified Copies (no older than 12 months) of Academic and Professional Qualifications should be attached.**	5 =Proposed engagement team collectively possesses **all** listed certifications 4 = Proposed engagement team collectively possesses 4 to 5 of the listed certifications 3 = Proposed engagement team collectively possesses 3 of the listed certifications 2 = Proposed engagement team collectively possesses 2 of the listed certifications 1 = Proposed engagement team collectively possesses 1 or 0 of the listed certifications	**20**

DOMAIN	EVALUATION METHOD	CRITERIA	WEIGHT
2. Experience of the proposed team (20)	Project Team Members should individually possess a minimum of 3 years experience in conducting Cybersecurity audits. *(Experience above the listed years to be an added advantage)* **NB: CVs detailing each members' qualifications and relevant experience should be attached**	5= Proposed team member possesses 6 years or more ICT audit experience. 4 = Proposed team member possesses 4 to 5 years' ICT audit experience. 3 = Proposed team member possesses 3 years' ICT audit experience 2 = Proposed team member possesses 2 years' ICT audit experience 1 = Proposed team member possesses less than 2 years' ICT audit experience **NB: Total score to be the average of all scores per engagement team member**	**20**

DOMAIN	EVALUATION METHOD	CRITERIA	WEIGHT
3. **Experience of Company / the Audit Firm**	The service provider must demonstrate, through submission of signed reference letters, completed **Cybersecurity Audits** over the past 10 years. Each letter must include the following information: • Client letterhead and name • Description of the project • The contact person, phone number / email address • Completed Project Period ***NB: Only the reference letters indicating all the requirements mentioned above will be considered.***	5 = 5 or more signed reference letters of completed **Cybersecurity Audits** in the past 10 years 4. = 4 signed reference letters of completed **Cybersecurity Audits** the past 10 years 3 = 2 to 3 signed reference letters of completed **Cybersecurity Audits** in the past 10 years 2. = 1 signed reference letter of completed **Cybersecurity Audits** in the past 10 years 1 = 0 signed reference letters of completed **Cybersecurity Audits** in the past 10 years	**30**

DOMAIN	EVALUATION METHOD	CRITERIA	WEIGHT
4. Membership with ISACA and EC-Council	At least 2 members of the proposed team members collectively have active memberships with ISACA and/ or the EC-Council. **NB: Membership Certificates or membership confirmation letters from relevant professional bodies indicating that memberships are the only acceptable evidence.**	5= At least 4 members of the proposed team collectively hold active ISACA and/or EC-Council memberships. 4 = At least 3 members of the proposed team collectively hold active ISACA and/or EC-Council memberships. 3 = At least 2 members of the proposed team collectively hold active ISACA and/or EC-Council memberships. 2 = Only 1 member of the proposed team hold active ISACA and/or EC-Council memberships 1 = 0 member of the proposed team hold active ISACA or E-Council memberships	**15**

DOMAIN	EVALUATION METHOD	CRITERIA	WEIGHT
5. Cybersecurity Audit Methodology	Provide a comprehensive cybersecurity audit methodology in line with relevant cybersecurity frameworks.	5= Provision of a comprehensive cybersecurity audit methodology referencing relevant cybersecurity frameworks. The methodology includes cybersecurity audit tools and techniques to be implemented by the bidder during audit reviews. 4 = Provision of a comprehensive cybersecurity audit methodology referencing relevant cybersecurity frameworks 3 = Provision of a cybersecurity audit methodology, with minimal or summarised referencing to relevant cybersecurity frameworks. 2 = A methodology has been provided, but it is not relevant to cybersecurity audits 1 = The proposal has no documented audit methodology.	**15**

Woodpecker Building | Hillcrest Office Park
177 Dyer Rd | Hatfield | Pretoria | 0083
Tel: +27 12 423 5700 | **Fax:** +27 12 423 5755/65
communications@pseta.org.za | www.pseta.org.za

PHASE 2:

The bids will be evaluated on the 80/20 principle with 80 points being allocated for price and 20 points allocated for specific goal, once the minimum functionality criteria are met.

Phase 2 evaluation will be based on the following:

		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

14.1 Proposals must be submitted physically to our PSETA offices

14.2 Submission of all applicable documents as indicated below:

i. Bidders who are claiming points for disability must submit as evidence of disability, a certified medical report/letter from the authorised body as well as a certified copy of doctor's certification with medical practice number.

ii. Certified copies of the director's ID's document (in order claim points for disability as per SBD 6.1,)

iii. Certified copy of BB-BEE certificate or sworn affidavit

iv. Valid Tax compliance status (TCS) PIN or proof of exemption from SARS;

v. Copy of the registration document of the organisation (CIPC);

vi. 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)
- **Three (3) or more proposals to be submitted (1x original hard copy and 2 or more copies/replicas)**

NB: Please note that failure to submit documents requested on section 15.1 will render the proposal disqualified.

Bid proposals must be submitted to: Lungile Mokoena

SCM Specialist (Acting) : Supply Chain Management

The PSETA

Ground Floor, Woodpecker Building, 177 Dyer Road, Hillcrest Office Park, Pretoria

No late applications will be accepted.

No electronic bid applications will be accepted.

The validity periods of the bids are 90 days from the closing date.

Please direct all queries to Ms. Lungile Mokoena via email on Lungilem@pseta.org.za

Vivian Selauli

Digitally signed by Vivian Selauli
Date: 2026.11.06 15:16:57 +02'00'