

THE PUBLIC SERVICE SECTOR EDUCATION TRAINING AUTHORITY

Terms of Reference

APPOINTMENT OF A SERVICE PROVIDER TO CONDUCT AN ASSESSMENT OF PSETA'S INFORMATION SECURITY SYSTEMS IN TERMS OF THE INTERNATIONAL ORGANISATION FOR STANDARDISATION ("ISO") 27001:2022 STANDARD.

RFP NUMBER.....

CLOSING DATE:

CLOSING TIME:



1. INTRODUCTION

The Public Service Sector Education and Training Authority (PSETA) is a Sector Education and Training Authority (SETA) established in terms of section 9(1) of the Skills Development Act 97 of 1998 as amended and is classified as a National Public Entity under schedule 3A of the Public Finance Management Act, 1 of 1999.

2. OBJECTIVES OF THE ASSIGNMENT

- 2.1. The PSETA seeks to strengthen its information security management systems and data protection within the Organisation. This entails complying with data privacy frameworks and assessing the controls currently in place for information security within the PSETA.
- 2.2. In order to improve its information security management systems and data protection, PSETA needs to procure a service provider that will conduct an assessment of its information security systems in terms of the International Organisation for Standardisation ("ISO") 27001:2022 standard.
- 2.3. Prospective bidders are invited to submit a detailed proposal to act as service providers for providing the envisaged services on behalf of PSETA on an on-going basis for a period not exceeding 08 months commencing from the date of signing the contract.

3. SCOPE OF WORK

The scope of work covers the following:

- 3.1. Conduct an assessment of PSETA's information management security needs in line with the ISO 27001:2022 standards.
- 3.2. Assessing the controls that PSETA has currently set up for information management systems and determining whether the controls comply with the ISO 27001:2022 standards.
- 3.3. A gap analysis of PSETA's information security management systems, where the assessment indicates that PSETA's systems do not meet the ISO 27001:2022 Standard.
- 3.4. Assisting the PSETA to achieve ISO 27001:2022 standard certification.

4. PROJECT DELIVERABLES

- 4.1. The purpose is to appoint a suitable, qualified, and competent service provider to assist PSETA in conducting an assessment of its information security systems in terms of the ISO/IEC 27001:2022 standard.
- 4.2. In order to manage risk, improve its controls for information management, and align the systems to international best practices, the PSETA needs to conduct an assessment of its information management security systems in accordance with the ISO 27001:2022 standard.
- 4.3. The appointed service provider will assist the PSETA with assessing PSETA's information security needs in terms of the ISO/IEC 27001:2022 standard.
- 4.4. Bidders should take note that there will be a compulsory briefing session for bidders.

5. COMPETENCIES AND SKILLS SET REQUIRED

The Service Provider should meet the following requirements:

- 5.1. The service provider should have an excellent and proven track record in conducting assessments of clients' information management security systems in accordance with the ISO 27001:2022 standards.
- 5.2. Assisting clients to achieve ISO 27001:2022 standard certification.
- 5.3. Providing training in information security management systems and how to improve the adequacy and effectiveness of such systems.

6. TIME FRAME

- 6.1. The appointed service provider's services will be required for 08 months from the date of appointment.
- 6.2. The project manager of the appointed Service Provider will report directly to the PSETA Deputy Information Officer, or any other delegated representative, as and when required.

7. COSTING

- 7.1 A cost analysis must be given to cover the full project amount. The proposed project pricing must be all-inclusive (i.e. including professional fees, venue hire, travel expenses, disbursements and VAT).
- 7.2. The PSETA may require a breakdown of rates on any of the items priced and service providers are required to provide same. PSETA reserves the right to negotiate the price.
- 7.3. Bidders should quote their rates on an hourly basis for the services, for each level of professional, in their proposals.

8 EVALUATION PROCESS

- 8.1 The bids 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.

PHASE 1: FUNCTIONALITY EVALUATION

- 8.2 Bids must meet the minimum eligibility criteria in respect of functionality of 65 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.

PHASE 2

- 8.3 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 1 – FUNCTIONALITY EVALUATION

Domain	Evaluation Method	Criteria	Weight
1. Company Profile and experience	Please provide company profile and signed reference letters for services related to	1 = no reference letter and/or company profile; 2 = one reference letter and company profile;	05

Domain	Evaluation Method	Criteria	Weight
	conducting an assessment of client's information security systems in terms of the ISO 27001:2022 standard, on client's letter head. (public sector or private sector clients)	3 = two reference letters and company profile; 4 = three reference letters and company profile; 5 = four to six reference letters and company profile; 6 = seven or more reference letters and company profile.	
2. Project Plan indicating readiness to implement and complete within required timeframes	Please submit a detailed project plan for the implementation of the project. The project must, at a minimum, contain the following: a) Detailed activities; b) Clear deliverables with timeframes for completing the deliverables; c) Roles and responsibilities allocated for the envisaged deliverables; d) The proposed timeframes must be within the overall duration of the project.	1 = Non submission of project plan; 2 = Project plan addresses 1-2 requirements in evaluation guide; 3 = Project plan addresses 3-4 requirements in evaluation guide; 4 = Project plan addresses 5 requirements in evaluation guide 5 = Project plan addresses 6 or more requirements in the evaluation and includes more proposed activities.	15
3. Knowledge and experience of the Project	Qualification(s) of Lead Professional/Project Manager who will be deployed to provide the envisaged service.	1 = Non submission of CV and/or certified copies of qualifications; 2 = CV, certified copies of qualifications and	30

Domain	Evaluation Method	Criteria	Weight
Manager/Lead Professional	The Lead Professional/Project Manager must: a) Have an appropriate academic qualification and at least 5-10 years of work experience regarding providing services pertaining to successfully assisting public sector and/or private sector organizations in conducting assessments of client's information security systems in terms of the ISO 27001:2022 standard. b) Attach a CV and certified copies of qualifications. Proof of SAQA evaluation must be provided in the case of foreign qualifications.	less than 5 years of experience; 3 = CV, certified copies of qualifications and 5 - 7 years of experience; 4 = CV, certified copies of qualifications and 8 - 10 years of experience; 5 = CV, certified copies of qualifications and more than 10 years of experience.	
4. History of successful implementation of similar projects.	Sample of report(s) done on behalf of clients wherein service provider conducted an assessment on behalf of client in public or private sector and outcomes and/or recommendations from the assessment. Sample report of ISO 27001:2022 assessment conducted should be of assessments previously done within the last seven (7) years on behalf of public or private sector clients. (the document may be abridged)	1 = no sample report or framework documents of similar projects previously done; 2 = 1 sample report or framework document of similar projects previously done; 3 = 2-3 sample reports or framework documents of similar projects previously done; 4 = 4-5 sample reports or framework documents of similar	50

Domain	Evaluation Method	Criteria	Weight
	(the identity of clients may be blacked out in order to protect personal information of such clients).	projects previously done; 5 = 6 or more sample reports or framework documents of similar projects previously done.	
Total			100

Phase 2: Price and Specific goals

Phase 1: Functionality evaluation		Points
Phase 2: Preferential Points system		
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

9 FORMAT OF THE BID SUBMISSION

- 9.1. Proposals must be submitted in physical copies: three (3) hard copies, comprising one (1) original and two (2) copies (replica of the original proposal).
- 9.2. Company profile indicating all the requirements as per the evaluation criteria.
- 9.3. Proposal with project plans and other specified requirements in the functionality section.
- 9.4. Reference letters.
- 9.5. Team member names and roles and certified copies of qualifications and CVs.
- 9.6. Sample documents of previous work done in conducting assessments of client's information security systems in terms of the ISO 27001:2022 standard.
- 9.7. Any other information or documentation specified in the functionality section.
- 9.8. Submission of all applicable documents as indicated below:
 - a) Certified copy of doctor's certification with medical practice number.
 - b) Certified copies of the director's ID's document(in order claim points for disability as per SBD 6.1)
 - c) Certified copy of BB-BEE certificate or sworn affidavit
 - d) Valid Tax compliance status (TCS) PIN or proof of exemption from SARS;
 - e) Copy of the registration document of the organisation (CIPC);
 - f) Copy of the Central Supplier Database registration.

10. IMPORTANT MANDATORY INFORMATION FOR BIDDERS

- 10.1. All Standard Bidding documents (SBD) documents must be completed and signed.
 - a) SBD 1 (All sections must be fully completed)
 - b) SBD 4 (All sections must be fully completed)
 - c) SBD 6.1(All sections must be fully completed)
 - d) Proof of registration on Central Supplier Database.
 - e) General Conditions of Contract (All pages must be signed or initialled)
- 10.2. Bidders should take note that there will be a compulsory briefing session for bidders.

NB: Please note that failure to submit documents requested on section 9 will render the proposal disqualified.

Proposals must be submitted to:

Ms. Ursula Mathonsi

Manager: Supply Chain Management

Public Service Sector Education and Training Authority (PSETA)

Woodpecker Building, 177 Dyer Road

Hillcrest Office Park, Hillcrest, Pretoria, 0083

Closing date:

Closing time: 11:00

The tender is valid for 120 days from the closing date.

Electronic documents will not be accepted.