SOUTH AFRICAN

CIVIL AVIATION AUTHORITY

Request for Quotation (RFQ) for Cyber Security Awareness Training for a period of three (3) years

SPECIAL CONDITION:

BIDDERS ARE REQUIRED TO SUBMIT THEIR BIDS ON TIME TO AVOID BEING LATE. OUR NEW OFFICE PARK HAS STRIGENT SECURITY MEASURES THEREFORE EACH BIDDER WILL BE REQUIRED TO MAKE A PRIOR ACCESS CODE ARRANGEMENT WITH BETTY ON 082 885 4270 OR SAM ON 071 473 5462.

Terms of reference
Request for Quotation for Cyber Security Awareness Training for a period of three (3) years

1. INTRODUCTION

The South African Civil Aviation Authority (SACAA) is an agency of the Department of Transport (DoT), established in terms of the Civil Aviation Act, 2009 (Act No.13 of 2009), which came into effect on 31 March 2010. The Civil Aviation Act provides for the establishment of a stand-alone authority, mandated with controlling, promoting, regulating, supporting, developing, enforcing, and continuously improving levels of safety and security throughout the civil aviation industry.

The SACAA's mandate is to administer civil aviation safety and security oversight in the Republic of South Africa, in line with Civil Aviation Authority Act (the Act), and in accordance with the Standards and Recommended Practices (SARPs) prescribed by the ICAO.

The above is achieved by complying with the SARPs of the ICAO, whilst considering the local context.

The SACAA, as prescribed by the Civil Aviation Act as well as the Public Finance Management Act (PFMA), 1999 (Act No.1 of 1999) is a Schedule 3A public entity.

2. INVITATION TO BID

The South African Civil Aviation Authority (SACAA) seeks to appoint a suitably qualified service provider to facilitate a Cybersecurity Awareness Workshop for 700 employees. The objective of this training program is to educate employees on cybersecurity risks and best practices, aiming to reduce the likelihood of human-related security incidents such as phishing and social engineering, while ensuring compliance with standards and frameworks including ISO 27001, NIST, ICAO cybersecurity guidelines, and local regulations like POPIA all while providing measurable outcomes to assess both knowledge retention and behavioral change.

The training aims to educate and train employees on cybersecurity best practices in the workplace to prevent security breaches. The workshop will be conducted virtually via Microsoft Teams

3. SCOPE OF WORK

The selected service provider will be responsible for:

- Delivering **12 cybersecurity awareness training sessions** over a period of three years.
- Conducting **one session per quarter**, each lasting **one hour**.
- Training **700 employees** on cybersecurity best practices to mitigate security risks.
- Covering key cybersecurity topics, including but not limited to:
    1. The need for cybersecurity
    2. Phishing, spear-phishing, and social engineering attacks
    3. Safe use of email, internet, and corporate applications
    4. Password management and multi-factor authentication
    5. Mobile device and remote work security
    6. Social media best practices and privacy awareness
- Data protection, privacy, and handling sensitive information Ensuring the training is interactive and engaging for all staff members.
- Providing training materials and recordings after each session for reference.
- Training must be conducted via Microsoft Teams
- The service provider must have experienced trainers with expertise in cybersecurity awareness.

Customisation

- Content should be tailored to a corporate environment and aligned with industry best practices.
- Tailoring content to reflect organisation-specific policies, procedures, and real-life scenarios
- Incorporating the organisation’s branding and messaging

- Inclusion of sector-specific threats, e.g., aviation/transportation cybersecurity risks

4. EVALUATION CRITERIA

Bidders will be evaluated in accordance with the Supply Chain Management Policies as well as the Preferential Procurement Policy Framework, 2000 (Act No. 5 of 2000) and the Preferential Procurement Regulations of 2022.

4.1. PHASE 1 – SUPPLY CHAIN MANAGEMENT (SCM) ADMINISTRATIVE MANDATORY COMPLIANCE REQUIREMENTS

Bids received will be verified for completeness and correctness. The SACAA reserves the right to accept or reject a bid based on the completeness and correctness of the documentation and information provided. The set of bid documents must be completed and submitted. (**SACAA reserve the right to request information/additional documents if there are any missing from the bidder(s) submission**).

Bidders are to ensure that they submit the following documentation / information with their bid.

Document	Comments	Compulsory requirement
Proof of registration on the Central Supplier Database (CSD) of National Treasury	Prospective bidders must be registered on the Central Supplier Database (CSD) prior to submitting bids. **Please indicate / supply the supplier number**.	Yes
SBD 4 (Bidders Disclosure)	Completed and signed	Yes

4.2 PHASE 2 - TECHNICAL AND/ OR FUNCTIONALITY EVALUATION

4.2.1 The following table is critical to the evaluators and will be a benchmark against your submission as per section 5 (1) of the Preferential Procurement Policy framework, Act 2000: Preferential Procurement Regulations, 2017.

Table 1: Functionality Evaluation

FUNCTIONALITY EVALUATION: Functionality Description			
Technical Requirements:	**Description**	**Min**	**Max**
Company profile	Five years's experience in conducting Cyber Security Awareness Training (Bidder must attach the Company profile stating the years of experience) 5 years' experience or more = **(30 points)**	**30**	**30**
Contactable references	Provide dated and signed letters of reference on client's letterhead, including the contact person and contact details from the entity from which services were rendered. Reference must be in relation to this type of service provided in the **last three (3) years.** • Three (3) contactable reference letters from clients where Cyber Security Awareness Training were provided in the past 3 years from the closing date of this RFQ – **(10 Points).** • Four (4) contactable trade reference letters from clients where Cyber Security Awareness Training were provided in the past 3 years from the closing date of this RFQ – **(20 Points).**	10	30

	• Five (5) contactable trade reference letters from clients where Cyber Security Awareness Training were provided in the past 3 years from the closing date of this RFQ – **(30 Points).**		
Project Leader's/Facilitators Qualification:	Provide certification Bachelor's Degree in Computer Science or equivalent	40	40
Total Points		**80**	**100**

Bidders who scores minimum of 80th points on functionality evaluation will be considered further for phase 3 which is Price and B-BBEE.

4.2 PHASE 3 – PRICE AND SPECIFIC GOALS EVALUATION

Bidders who comply with the requirements of this bid will be evaluated according to the preference point scoring system as determined in the Preferential Procurement Regulations, 2022 pertaining to the Preferential Procurement Policy Framework Act, (Act No 5 of 2000).

For this bid 80 points will be allocated for Price and 20 points for Specific Goal.

4.2.1 This tender will be evaluated using the 80/20 preferential point system. The following PPPFA formula will be used to evaluate price:

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

Ps = Points scored for price of the bid under consideration.

Pt = Rand value of bid under consideration.

Pmin = Rand value of lowest acceptable bid.

Only bidders that have achieved the minimum qualifying points on functionality will be evaluated further in accordance with the 80/20 preference point system as follows:

Points for this bid shall be awarded for:

(a) Price; and

(b) Specific Goal.

The maximum points for this bid are allocated as follows:

	POINTS
PRICE	**80**
SPECIFIC GOAL	**20**
Total points for Price and SPECIFIC GOAL	**100**

POINTS AWARDED FOR A SPECIFIC GOAL

In terms of the Preferential Procurement Regulations 2022, points will be awarded for specific goal in accordance with the table below:

SPECIFIC GOALS	**Number of points**
100% Black ownership	20
51% Black ownership	10
50 - 30% Black ownership	5
0% Black ownership	0

5 NON-COMPULSORY BRIEFING SESSION

There will be no briefing session and any service provider that may seek further clarity can send their queries to caaquotes@caa.co.za to seek any clarity on the tender document. All requests must be submitted through email.

6 SUBMISSION OF BID DOCUMENT

The bid submission requires a three (3) envelope system as per the evaluation criteria above.

1.1.1. Envelope 1

- All mandatory documents on Phase 1.

1.1.2. Envelope 2

- Technical proposal.

1.1.3. Envelope 3

- The pricing schedule must be submitted on a separate envelope from the technical proposal for ease of evaluation, as these will be evaluated separately. Bidders are required to provide a detailed price schedule breakdown as indicated in "**Annexure A**" below.

5. Bidders are required to submit neat and bounded documents, as SACAA will not be held responsible for any loss of documents whatsoever.

6. Bid documents shall be submitted in a sealed envelope and/or package clearly marked with the bid reference number as per the bid advert, bidder company name and be deposited in the tender box situated at the foyer of the SACAA head office, and be addressed as follows:

All bids submissions should be deposited or delivered at our Tender Box on or before 11:00am on the closing date of 29 September 2025.

Annexure A
Pricing Schedule

Item	Description	Quantity	Unit Price Excl. Vat	Total Price Excl. Vat
1	Group Virtual Cyber Awareness Training/ Workshop	12		
			Total Price Excluding VAT	
			15% VAT	
			Total Price Including VAT	