

**Postal Address**  
P.O. Box 1329, Rivonia  
2128, South Africa

**Physical Address**  
270 George Road,  
Noordwyk, Midrand, 1687

**Contact**  
**Call Centre:** 0860 100 221  
**Telephone:** 011 217 0600  
**Fax:** 011 783 7745



## SERVICES REQUISITION FORM

**YOU ARE HEREBY INVITED TO SUBMIT A QUOTATION FOR THE CULTURE ARTS,  
TOURISM, HOSPITALITY AND SPORT SECTOR EDUCATION AND TRAINING AUTHORITY  
(CATHSSETA)**

<b>Date issued:</b>	<b>31 October 2023</b>	<b>RFQ number</b>	<b>RFQ/COS/057/2023</b>
<b>Closing Date:</b>	<b>08 November 2023</b>	<b>Closing Time:</b>	<b>11H00am</b>
<b>DESCRIPTION:</b>	<b>PROVISION OF ICT SERVICES SUPPORT FOR A PERIOD OF 6 MONTHS</b>		

### 1. BACKGROUND

- 1.1 The Culture, Arts, Tourism, Hospitality and Sport Sector Education and Training Authority (CATHSSETA) is a Schedule 3A Public Entity established in terms of the Skills Development Act 97 of 1998 as amended (SDA). Its headquarters are situated at 270 George Road, Noordwyk in Midrand and the regional offices are in Cape Town and Durban.
- 1.2 CATHSSETA's mandate is to promote and facilitate skills development within our six (6) subsectors, namely, Arts, Culture and Heritage, Conservation, Gaming and Lotteries, Hospitality, Sport, Recreation and Fitness, and Tourism and Travel Services. CATHSSETA is one of the 21 Sector Education and Training Authorities (SETAs) across the economy mandated to deliver on the National Skills Development Plan (NSDP) outcomes.

- 1.3 CATHSSETA has a staff component of seventy-seven (77) employees. The Information and Communication and Knowledge Management Unit has four (4) staff members.

## 2. PURPOSE

- 2.1. CATHSSETA is seeking the services of an external service provider to support and maintenance for six (6) months to enhance and ensure the robustness of its Information and Communication Technology (ICT) cybersecurity, internal controls, and governance practices. The increasing complexity of ICT systems and the evolving threat landscape necessitate a comprehensive and proactive approach to cybersecurity and risk management.

## 3. SCOPE OF WORK

The scope of work for the external service provider shall include, but not be limited to the following:

### 3.1. ICT Cybersecurity Assessment:

- 3.1.1. Conduct a thorough assessment of existing ICT infrastructure, systems, and applications to identify potential cybersecurity vulnerabilities and weaknesses.
- 3.1.2. Evaluate the effectiveness of current cybersecurity measures and protocols in place.
- 3.1.3. Identify emerging threats and recommend mitigation strategies.

### 3.2. **ICT Internal Controls Review:**

- 3.2.1 Assess the organisation's current internal control framework related to ICT processes and data management.
- 3.2.2 Identify gaps or deficiencies in the internal controls that could lead to security breaches or non-compliance.
- 3.2.3 Implement improvements to strengthen internal controls and data integrity.

### 3.3. **ICT Governance Enhancement:**

- 3.3.1. Review the CATHSSETA's ICT governance structure, policies, and procedures.
- 3.3.2. Review the following draft policies to further enhance cybersecurity within the CATHSSETA environment.
  - Antivirus policy
  - Patch management policy
  - User account management policy
- 3.3.3. Evaluate the alignment of ICT strategies with the overall business objectives.
- 3.3.4. Provide recommendations to enhance ICT governance and ensure effective decision-making processes.

### 3.4. **Cybersecurity Solutions Implementation:**

- 3.4.1. Based on the assessment, propose, and implement cybersecurity solutions to address identified vulnerabilities.
- 3.4.2. Assist in configuring and deploying security tools and technologies.

3.4.3. Provide guidance on incident response and recovery planning.

#### **4. DELIVERABLES**

The Service Provider will be responsible for delivering the following:

- 4.1. Comprehensive assessment reports detailing cybersecurity vulnerabilities, internal control gaps, and governance recommendations.
- 4.2. Penetration testing reports highlighting vulnerabilities and recommended mitigation strategies.
- 4.3. Documentation of policies, procedures, and guidelines related to ICT cybersecurity, governance, and email anti-phishing.
- 4.4. Training materials for staff to raise awareness of cybersecurity best practices, internal controls, and email security.

#### **5. SERVICE PROVIDER REQUIREMENTS/COMPETENCIES**

- 5.1. Provide CVs and certified qualifications of the human resources; indicating knowledge, capability to deliver on the scope of work to organisations. Service provider must have One (1) Security Engineer that has at least three (3) years' experience on Cybersecurity and penetration testing; One (1) ICT Auditor with Certified Information Systems Auditor (CISA) qualification or equivalent responsible for ensuring that an organisation's IT systems are secure, reliable, and compliant with relevant laws and regulations and a Project Manager with at least five (5) years' experience in implementing similar projects.
- 5.2. Proven expertise in cybersecurity with a strong track record of assessing and mitigating cybersecurity risks.
- 5.3. Extensive experience in evaluating and enhancing internal controls within complex ICT environments.

- 5.4. Familiarity with industry standards and frameworks such as International Organisation for Standardisation (ISO) 27001 (Information Security Management), National Metrology Institute of South Africa (NMISA) Cybersecurity Framework, and Control Objectives for Information and Related Technologies (COBIT).
- 5.5. Strong communication skills to effectively collaborate with CATHSSETA's stakeholders.

## **6. REPORTING**

- 6.1. The service provider will report to the Information and Communications Technology and Knowledge Management Manager on all aspects of the contract performance.

## **7. COSTING**

- 7.1. All the projects and implementation costs must be provided as per specified requirements. Technical support costs for six (6) months must be provided for the IT Service provider submission.
- 7.2. The price quoted by the prospective service provider must include Value Added Tax (VAT).

## **8. CONDITIONS OF CONTRACT**

- 8.1. Support and maintenance costs for six (6) months must be provided for IT Service provider submission.
- 8.2. A Service Level Agreement (SLA) shall be signed with the preferred service provider.
- 8.3. The CATHSSETA reserves the right to invite short listed service providers to present their proposals for final decision. CATHSSETA will:



- 8.3.1. Provide documentation of the current infrastructure.
- 8.3.2. Provide access to the current infrastructure.
- 8.3.3. Provide the current organogram; and
- 8.3.4. Manage and monitor the delivery of services in accordance with the signed SLA.

## **9. EVALUATION CRITERIA**

### **9.1. Stage 1: Mandatory Requirements**

Compliance evaluation – service provider will first be evaluated in terms of compliance that is meeting minimum requirements. Service provider who does not fulfil all the requirements or do not submit required documents using the required format, will be disqualified and not move onto the next stage of evaluation.

### **Stage 2: Functionality Evaluation**

A Service provider is required to achieve a minimum point of **75**, failure to achieve the minimum points will lead to disqualification.

### **Stage 3: Price and Specific Goals Evaluation**

The quote will be evaluated in accordance with the 80/10 preference point system, minimum of 75 points must be achieved to qualify for evaluation on **Price** and **Specific Goals**.

The contract will be awarded to the bidder that scores the highest total number of points.

## FUNCTIONALITY EVALUATION

EVALUATION CRITERIA	SUB-EVALUATION CRITERION	WEIGHT
<b>1. A detailed technical proposal in line with the Scope of Work.</b> Clearly define: <ul style="list-style-type: none"> <li>• Cost breakdown;</li> <li>• Delivery timelines;</li> <li>• Resources responsible for implementation of the ICT Service Provider submission;</li> </ul>	Comprehensive responsiveness to all three (3) aspects of the technical proposal requirements	<b>30</b>
	Partial responsiveness to all three (3) aspects of the technical proposal requirements	15
	Not responsive to all three (3) aspects of the specification requirements outlined	0
<b>2. Knowledge and Expertise</b> Provide details of similar projects accomplished with the minimum of five (5) contactable references within the past (five) 5 years. Letters must be on the letterhead of the service provider and must be relevant to this project and specify year/month of service.	5 and more reference letters	<b>30</b>
	3 reference letters	15
	1 reference letter	5
	0 reference letter/No reference letter	0
<b>3. Expertise and knowledge of the company.</b> Please provide CVs and certified qualifications of the human resources; indicating knowledge, capability to deliver on the scope of work to organisations.	A team consisting of: <ul style="list-style-type: none"> <li>• Certified Security Engineer that has at least three (3) years' experience in Cybersecurity and penetration testing;</li> <li>• One (1) ICT Auditor with Certified Information Systems</li> </ul>	<b>40</b>

EVALUATION CRITERIA	SUB-EVALUATION CRITERION	WEIGHT
	<p>Auditor (CISA) qualification or equivalent and at least three (3) years' experience in the ICT auditing space;</p> <ul style="list-style-type: none"> <li>Project Manager with at least five (5) years' experience in implementing similar projects.</li> </ul> <p>A team consisting of:</p> <ul style="list-style-type: none"> <li>Certified Security Engineer with less than three (3) years in implementation of EDMS/E-Submission.</li> <li>One (1) or no ICT Auditor with CISA qualification or equivalent and less than three (3) years' experience in the ICT auditing space;</li> </ul> <p>Project Manager with less than five (5) years on implementation of similar projects</p>	<b>10</b>

**Bids that do not meet the minimum qualifying score for functionality will be eliminated from further evaluation.**

## **10. CONTRACT PERIOD**

10.1. The period of the project shall be six (6) months.

## **11. ADMINISTRATIVE REQUIREMENTS**

- Quote/Pricing with a clear breakdown of Scope with total inclusive of VAT.
- Completed and signed SBD4, SBD 6.1



**Postal Address**  
P.O. Box 1329, Rivonia  
2128, South Africa

**Physical Address**  
270 George Road,  
Noordwyk, Midrand, 1687

**Contact**  
**Call Centre:** 0860 100 221  
**Telephone:** 011 217 0600  
**Fax:** 011 783 7745



- 
- Valid Tax Compliance Pin issued by SARS.
  - Valid B-BBEE Certificate or Sworn Affidavit.
  - All RFQ related responses must include the RFQ number as the subject matter.
  - Central Supplier Database (CSD) Supplier Number.

**E-mail responses to [supplychain@cathsseta.org.za](mailto:supplychain@cathsseta.org.za) on or before the closing date and time as stated above.**