Terms of Reference (ToR)

Consulting Services for Cybersecurity and Network Security Expert

General Information

Project Name:	African Union Commission for Building Institutions and Systems to Harness and Realize Agenda (BIASHARA) 2063
Project ID:	180117
Consultancy name:	Consulting Services for Cybersecurity and Network Security Expert to Conduct AfCFTA Cybersecurity Assessment
Procurement Reference :	ET-AFCFTA-485255-CS-INDV
Type of Contract:	Individual Consultant Selection
Reporting to:	Administration and Human Resources Management Director
Duration of Assignment:	Sixty (60) Working Days

1. Introduction

1.1. These Terms of Reference (ToR) have been prepared to engage an Individual Consultant to undertake Consulting Services for Cybersecurity and Network Security assessment. The engaged expert will conduct AfCFTA Cybersecurity Assessment ensuring the security of AfCFTA network environment, recommend robust cybersecurity measures to protect sensitive data and maintain the integrity of its digital infrastructure.

2. Background

2.1. The AfCFTA Secretariat has received a grant to finance the Institutional Support Project for the effective implementation of the AfCFTA. The AfCFTA Secretariat is a pan-African organisation legally established and mandated to implement the AfCFTA Agreement, whose main objective is to create a single continental market for goods and services so to deepen the economic integration of the African continent, in accordance with the Pan African Vision of “An integrated, prosperous and peaceful Africa” enshrined in Agenda 2063.

2.2. The AfCFTA Secretariat serves as the central institution responsible for the implementation of the AfCFTA Agreement and its related Protocols. Its core functions encompass the facilitation of seamless, predictable, and liberalized trade among State Parties across the African continent through the implementation of dedicated support programmes.

3. Context

3.1 The AfCFTA Secretariat is committed to ensuring the security of its digital infrastructure, IT network environment and IT systems and is eager to implement robust cybersecurity measures to protect sensitive data and maintain the integrity of its digital infrastructure.

3.2 Despite operating in an environment where IT security is not the primary focus, the Secretariat recognizes the critical importance of safeguarding its network against potential cyber threats. This includes adopting best practices in cybersecurity, continuously monitoring vulnerabilities, and ensuring compliance with international security standards. By taking these steps, the AfCFTA Secretariat aims to create a secure and resilient IT environment that supports its mission of facilitating free trade across the African continent.

4. Objective

4.1 The general objective of this assignment is to hire a highly skilled cybersecurity and network security expert to conduct a thorough and comprehensive cybersecurity risk assessment and network security assessment for the AfCFTA's digital infrastructure, network environment, IT systems, and policies. The goal is to identify vulnerabilities and weaknesses in the current technical infrastructure, policies and practices and provide prioritized recommendations for improvement.

The hired expert will be expected to:

a) Assess the Current Cybersecurity Infrastructure, Policies, and Practices:

- Conduct a detailed review of the existing cybersecurity infrastructure, including hardware, software, and network components.
- Evaluate the current cybersecurity policies and procedures to ensure they align with the best practices and industry standards. In absence of any such policies and procedures to make recommendations for introduction and provide guidance on any gaps.
- Analyze the effectiveness of existing security measures and controls in place to protect against cyber threats.

b) Evaluate AfCFTA's Network Security Architecture, Configuration, and Defenses:

- Examine the network security architecture to ensure it is robust and capable of defending against potential cyber-attacks.
- Assess the configuration of network devices such as routers, switches, firewalls, and intrusion detection/prevention systems.

- Evaluate the effectiveness of network defenses, including perimeter security, internal network segmentation, and endpoint protection.

c) Identify Gaps, Vulnerabilities, and Risks in IT Systems, Networks, and Data Handling:

- Perform vulnerability assessments to identify security gaps and weaknesses in IT systems and networks.
- Analyze data handling practices to ensure sensitive information is adequately protected and complies with data protection regulations.
- Identify potential risks associated with third-party vendors and external connections to the network.

d) Provide Prioritized, Practical, and Cost-Effective Recommendations for Mitigating Associated Risks and Enhancing IT Systems, Networks, and Data Handling:

- Develop a comprehensive risk mitigation plan that includes short-term, medium-term, and long-term recommendations.
- Recommend feasible network security solutions such as Network Detection and Response (NDR), Network Access Controls (NAC), or Identity Access Management (IAM) to enhance security.
- Ensure that recommendations are practical, cost-effective, and aligned with the organization's budget and resources.

e) Deliver a Cybersecurity Awareness Session for AfCFTA Staff:

- Develop and deliver a cybersecurity awareness program tailored to the needs of AfCFTA staff. Thereafter AfCFTA Secretariat will be responsible for the implementation of the developed program.
- Conduct an interactive and engaging cybersecurity awareness session for all staff members aligned with AfCFTA cybersecurity policies and procedures (as updated, or to-be established through this consultancy). This will be a half-day hybrid session, and all associated costs will be covered by the AfCFTA Secretariat.
- The awareness session should cover key topics such as recognizing phishing attacks, safe internet practices, password management, and data protection; and provide practical tips and guidelines to help staff protect themselves and the organization from cyber threats.
- Advise on how to promote a culture of cybersecurity awareness and best practices throughout the organization.

5. Detailed Scope of Work

The expert will be responsible for the following tasks, ensuring a thorough and comprehensive assessment of AfCFTA's cybersecurity and network security:

5.1: Reviewing Existing IT Network Architecture

- **Endpoints**: Examine all endpoint devices including computers, mobile devices, and IoT devices to ensure they are properly secured and configured.
- **Firewalls**: Review firewall configurations and rules to ensure they are effectively protecting the network from unauthorized access and cyber threats.
- **Switches**: Assess the configuration and security of network switches to ensure proper segmentation and protection of network traffic.
- **Wi-Fi Network Environment**: Evaluate the security of Wi-Fi networks, including encryption methods, access controls, and the use of secure protocols.
- **Internal Systems**: Review the security of internal systems, including servers, databases, and applications, to ensure they are protected against vulnerabilities and threats.

5.2: Identifying Configuration Weaknesses, Outdated Network Architectures, or Poor Access Practices:

- **Configuration Weaknesses**: Identify any misconfigurations in network devices and systems that could lead to security vulnerabilities.
- **Outdated Architectures**: Assess the network architecture to identify outdated components that may not meet current security standards.
- **Access Practices**: Evaluate access control practices to ensure that only authorized personnel have access to sensitive systems and data.

5.3: Evaluating Existing Cybersecurity Policies, Procedures, and Practices:

- **Policies**: Review existing cybersecurity policies, or gaps thereof, to ensure they are comprehensive and aligned with best practices.
- **Procedures**: Evaluate the procedures in place, or gaps thereof, for managing cybersecurity incidents, including detection, response, and recovery.
- **Practices**: Assess the day-to-day cybersecurity practices, or gaps thereof, of staff to ensure they are following established policies and procedures.

5.4: Evaluating Password Policies and Data Protection Mechanisms:

- **Password Policies**: Review password policies to ensure they require strong, complex passwords and regular updates.

- **Data Protection Mechanisms**: Assess the mechanisms in place for protecting sensitive data, including encryption, access controls, and data masking.

5.5: Assessing Data Security and Backup Systems:

- **Data Security**: Evaluate the security measures in place to protect data at rest and in transit, including encryption and secure storage solutions.
- **Backup Systems**: Review the backup systems to ensure they are reliable, regularly tested, and capable of restoring data in the event of a cyber incident.

5.6: Identifying Vulnerabilities and Potential Risks in the Organization's Systems:

- **Vulnerability Assessment**: Conduct vulnerability assessments to identify weaknesses in systems, applications, and network devices.
- **Risk Analysis**: Perform a risk analysis to identify potential threats and the impact they could have on the organization.

5.7: Delivering a detailed Report:

- **Risk Assessment**: Provide a comprehensive risk assessment that identifies potential threats and vulnerabilities.
- **Identified Weaknesses**: Detail the weaknesses found in the network and IT systems.
- **Recommendations for Improvements**: Offer practical, prioritized recommendations for improvements, categorized into short-term, medium-term, and long-term actions.

5.8: Conducting a Hybrid Staff Awareness Session:

- **Awareness Session**: Conduct a cybersecurity awareness session for AfCFTA staff, using a hybrid approach that includes both in-person and virtual components.
- **Training Content**: Cover key topics such as recognizing phishing attacks, safe internet practices, password management, and data protection.
- **Interactive Elements**: Include interactive elements such as quizzes, case studies, and Q&A sessions to engage staff and reinforce learning.

Note: It is indicated under the objectives on 4.(e) that This will be a half-day hybrid session, and all associated costs will be covered by the AfCFTA Secretariat.

6. Deliverables

6.1: Inception Report and Work Plan

- Outline project objectives, methodology, detailed work plan, resource allocation, and risk management plan.

6.2: Cybersecurity and Network Security Assessment Report

- Provide preliminary findings, identified vulnerabilities, detailed recommendations, and develop an implementation plan

6.3: Improve and/or Develop Cybersecurity Policies, Manuals, Templates and Forms

- Update and improve existing Cybersecurity, or develop new comprehensive policies, manuals, templates, and forms by conducting thorough research, engaging stakeholders, drafting documents, and ensuring compliance with international standards.

6.4: Provision of Cybersecurity Awareness Session to All Staff

- Conduct a hybrid session (in-person and virtual) covering, *inter alia*, phishing attacks, safe internet practices, password management, data protection, and incident reporting. It will include interactive elements, and the provision of training materials aligned with AfCFTA cybersecurity policies and procedures (as updated, or to-be established through this consultancy).

7. Evaluation and Qualification Criteria

7.1. Interested individuals should provide information on their qualifications and experience demonstrating their ability to undertake the assignment (CV and testimonials in form of contracts or reference letters or completion of service certificates as proof of similar assignments) and technical proposal outlining the technical approach and methodology for delivery of the assignment.

7.2. Shortlisted consultants will be evaluated on the following criteria based on the information provided in their CV, copies of certificates, testimonials and technical proposal.

#	Qualifying Criteria	Points
1	**General Education, Qualification and Relevant Training.** Consultant to indicate the name and type of degree obtained, the year of the degree and must attach copies of certificates to support qualification. • Relevance, including certification – 15% • Attached certificates – 5%	**20**
2.	**Relevant Experience** a) **Industry Experience**: A minimum of Seven (7) years of professional experience in cybersecurity risk assessment, mitigation, and network security assessment. (12.5%) b) **Diverse Clientele Support**: Proven experience in supporting a diverse range of international clients, including governments, non-governmental organizations, and the private sector. (12.5%)	**50**

	c) **Cyber Threat Knowledge**: Demonstrated knowledge and in-depth understanding of current cyber threats, vulnerabilities, and application of best practices in cybersecurity. (12.5%) d) **Cybersecurity training tools:** Demonstrated use and application of various cybersecurity training tools and techniques, such as simulations, hands-on exercises, and online training platforms (12.5%)	
3.	**Technical Approach and Methodology:** • Demonstrated understanding of the assigning (6%) • Work plan (6%) • Objectives (6%) • Activities (6%) • Deliverables (6%)	**30**
TOTAL		**100**

7.3. The minimum technical qualification is 80%. The consultants meeting the minimum technical qualification will be ranked and the first on the list will be invited for negotiation and subsequently be selected for the assignment if his/her fee rate is within the budget.

8. Qualifications and Experience

8.1 Qualifications:

The consultant must have a minimum degree in Computer Science, Computer Engineering, Software Engineering or Information Technology.

Professional certification in any of the following is desirable.

- Certified Information Systems Auditor (CISA)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified Ethical Hacker (CEH)
- ISO/IEC 27001 Lead Auditor/Implementor
- Cisco Certified Network Professional Security (CCNP Security)

8.2 Experience

This consultancy is open to experts who meet the following criteria:

a) Experience in leading cybersecurity projects and possess knowledge of global best practices in cybersecurity policy development.

b) Held position of cyber security expert in a private / public organization or acted in capacity as Cybersecurity consultant on separate projects like this one.
c) Demonstrated implementation of projects similar to this assignment.
d) Excellent communication skills, and experience in managing projects in this context. Fluency in English is mandatory, with recognized second language of the African Union preferred.

9. Assignment technical approach and methodology

The consultant is required to prepare and submit a clear and simple but detailed technical approach and methodology demonstrating his/her understanding of the assignment while also outlining his/her work plan, objectives, activities, deliverables and output relevant to the assignment. If necessary, the consultant may also be required to indicate activities which will require physical engagement and those that will require virtual engagement and these should also be included in the technical proposal submitted by the consultant.

10. Duration

The assignment will be for 45 consulting days over a 3-calendar month duration. The assignment will combine home-based and at least 2 x 2-week periods of onsite work.

Resources to be provided by the Client

The hired expert will be provided with the working space at AfCFTA Secretariat office where applicable, as well as internet access. All related expenses of venue, equipment, refreshments (where applicable) for delivery of awareness session detailed in the scope of work are to be provided by the AfCFTA Secretariat. Travel and assignment expenses will be reimbursable costs payable upon presenting authentic receipts.