AFRICAN UNION
الاتحاد الأفريقي

UNION AFRICAINE
UNIÃO AFRICANA

P. O. Box 3243, Addis Ababa, ETHIOPIA Tel.: (251-11) 5517700 Fax: (251-11) 5517844
www.au.int

African Union

Request for Quotations

(FOR SERVICES)

Consultancy for Provision of Training Service for cyber security based on Open source tools
EC-COUNCIL Certified Ethical Hacking (CEH) and Certified Information System Security Professional (CISSP)

22 October, 2018

Procurement number: AUC/AHRM/MIS/T/167

October 2018

The African Union Commission invites you to submit your quotation for providing Training services as described herein. Any resulting order shall be subject to the standard AU contract.

Bidders are required to furnish the following:

- Registration Certificates and Business Licenses
- Proof of having performed similar services in the previous 3 years

A firm will be selected under **Quality and Cost Based Selection *Method*** and procedures described in this EOI.

Bid Submission modalities and submission deadline: This is a two envelope bidding. **For manually submitted bids,** bidders should ensure that the **Technical and Financial proposals** are enclosed in **TWO separate envelopes** sealed and both should be enclosed in one Outer envelope clearly indicating the title and Procurement number.

For email submissions, please ensure that the technical and Financial proposals are attached as separate files. The subject of the email must clearly specify the title of the Consultancy.

Proposals must be submitted no later than Friday, 9th November 2018 at 15:00hrs.

Address for Bid submission:

The Chairperson of the Tender Board
African Union Commission, Roosevelt Street,
Building C, 3rd Floor, P.O. Box 3243, Addis Ababa, Ethiopia
Tel+251 115517700; Email; **tender@africa-union.org**

Clarification Requests: Clarification requests should be addressed to **tender@africa-union.org,** Tel+251115517700, **Ext 4321**

Yours Sincerely

Carine Toure Yemitia (Mrs)
Head of Procurement, Travel and Stores Division

Call for Proposals to Design and Deliver a Training on: Cyber-security based on Open source tools and Management of Information System: EC-COUNCIL CEH and CISSP

1. Introduction

In pursuit of its mandate to ***ensure the best quality of service for IT support,*** the Management of Information System (MIS) would like to conduct a training session on a duration of two weeks on: Cyber-security based on Open source tools and Management of Information System: **EC-COUNCIL CEH and CISSP** in the month of November 2018.

2. Justifications for the need for these trainings.

The following are the basis for the immediate need for these trainings:

2.1. Cyber security and Open source tools and Management of Information System:

Cyber security is a matter focusing attention of African Union's top management. Various assessments have shown evidence about the weaknesses of our infrastructure in terms of:

- Networking infrastructure;
- System infrastructure;
- Telephony system
- SAP/ERP and application developments.

Cyber-security is the protection of network-connected systems, including hardware, software and data, from cyber-attacks. In a computing context, security comprises cyber-security and physical security -- both are used by enterprises to protect against unauthorized access to data centres and other computerized systems. Information security, which is designed to maintain the confidentiality, integrity and availability of data, is a subset of cyber-security.

AU needs to increase the skills of its IT resources in order to cover the main issues that can have a huge impact on the business continuity. To achieve this goal, various tools are available on the market, unfortunately most of them are very expensive. That is the reason why the Open source tools, released under free licenses, can be an alternative.

It is therefore, found indispensable to organize a training session on Cyber-security based on Open source tools for the staffs of MIS and other IT resources disseminated in other departments, as well as other AUC staff members using /intending to use or deal with Cyber-security tools.

2.1.1. Course overview –

The course is targeted for beginners of Linux system administrators, Kali Linux and other Open source tools, who are interested in learning essential system administration skills, security best practices for web-services, network, systems and applications developments by following the training module **Ethical Hacking of EC-Council**. The class provides-hands-on training to effectively use, customize, and script common command line utilities. In addition, administrators will learn how to perform essential system administration tasks including basic installation, package management, user management procedures, security advises and best practices, security vulnerabilities and countermeasures.

2.1.2. Audience

• Microsoft® Windows users and system administrators who wish to learn more about Cyber-security

• IT professionals who want to build user-level Linux skills and learn fundamental system administration skills
• Network administrators, database administrators, applications developers, and others who have worked on other operating systems but now want to perform those tasks on a Linux system.

2.1.3. Prerequisites

• User-level experience with any computer operating system; Prior command-line experience is helpful but not required course content
• Linux ideas and history; Running commands and getting help
• Browsing the file system; Users, groups, and permissions
• Using the bash shell; Standard I/O and pipes
• Text processing tools and editors; Investigating and managing processes
• Finding and processing files; Network clients, Essential system administration tools
• Networking TCP/IP protocols
• Security vulnerabilities…

3. Target Participants

The training will target twenty (20) staff members from, but not limited to, MIS, the Knowledge Management (KM) Divisions, the Peace and Security department, as well as other departments.

4. Objective of the training

The objective of this training is to expose participants to the knowledge of Cyber-security best practices and countermeasures techniques to efficiently and effectively manage an Enterprise IT infrastructure; and discharge their individual and collective responsibilities in their area. Besides, it is expected to motivate staff members to be innovative, beyond finding solutions to the challenges encountered while executing their daily tasks.

5. The African Union Commission will:

a. Provide the venue, flip charts, and projector.
b. Provide administrative support, assist the trainer for trainees full participation in the training

6. Qualification and Experience of the training Provider

- The Trainers / Team members need to have International relevant experiences and wide ranges of practical work and teaching experiences in Cyber-security and Linux based solutions.
- The Trainers / Team members need to have a certification on **EC-Council Ethical Hacking and CISSP**
- They must have a minimum of 5-7 years' related experience.
- Excellent English language is mandatory. Knowledge of French will be an added advantage/asset.

7. Deliverables

7.1. Producing a team of experts in Linux based and Open source tools oriented to Cyber-security and new Certified Ethical Hacker at AUC:

- Working knowledge in Cyber-security;
- Working skills developed in Linux/Kali and others Open source tools;
- Step by step working manual, and Power Point Presentation;
- Issue certificates to participants at the end of the training session.

8. Desired Outcome

By the end of the training, it is expected that the trainees will have the skills required in:

- Using Linux/Kali Open Source tools and other tools to detect and prevent an attack.

- Identify the most common Cyber-security vulnerabilities and deploy countermeasures.

9. Training modules details CEH

Training Topic	participants	Duration	Language	Venue
Introduction to Ethical Hacking	20	5 days	English	AU Headquarters
Footprinting and Reconnaissance				
Enumeration and vulnerability analysis				
System hacking and countermeasures				
Malware Threats, Sniffing				
Social engineering attacks				
Evading IDS, Firewalls, Honeypots and countermeasures				
Web application security and SQL Injection				
Hacking Wireless Networks				
Hacking Mobile Platforms				
IoT Hacking				
Cloud Computing security				
Security of mobile devices and countermeasures				

10. Training modules details CISSP

Training Topic	participants	Duration	Language	Venue
Cyber Security and risk management	20	5 days	English	AU Headquarters
Assets protection				
Security engineering				
Identity management				
Network and telecommunication security				
Evaluation and security test				
Security of domain				
Security of development				

11. Resume of needs requested for quotation

Training session	Duration	Participants	Certification vouchers
Certified Ethical Hacking training (CEH)	**5**	**20**	**10**
Certified Information Systems Security Professional (CISSP)	**5**	**20**	**10**

12. Evaluation Criteria

a) Relevant international experiences in Cyber-security – 30 points;
b) Relevant experiences in training on Open sources technology – 30 points;
c) Diplomas and certifications of the trainer(s) - Ethical Hacking certification and CISSP- 20 points
d) Methodology and approach (understanding of the TOR, curriculum and) – 20 points

On the basis of the above combined evaluation factors, the technical evaluation will have a total weight of 70% and then the financial proposals will be considered with a weight of 30%.

Financial Proposals

Firms must submit detailed breakdown of the financial proposal entailing but not limited to:

a) Professional fees
b) Training/content preparation
c) Reimbursables (e.g travel, DSA etc)