EAST AFRICAN COMMUNITY

TERMS OF REFERENCE FOR CONDUCTING CYBER SECURITY AUDIT AND A RISK ASSESSMENT FOR ICT INFRASTRUCTURES AND SYSTEM FOR THE 50 MILLION AFRICA WOMEN SPEAK PROJECT AT COMESA HEAD OFFICE, LUSAKA, ZAMBIA.

EAC SECRETARIAT

Arusha, Tanzania

June 2020

TERMS OF REFERENCE FOR CONDUCTING CYBER SECURITY AUDIT AND A RISK ASSESSMENT FOR ICT INFRASTRUCTURES AND SYSTEM FOR THE 50 MILLION WOMEN PROJECT HOSTED IN COMMESA HEAD OFFICE.

I. Background of the assignment

The African Development Bank collaborated with Common Market for Easter and Southern Africa (COMESA), East Africa Community (EAC) and Economic Commission for West African States (ECOWAS) through the 50 Million Women Speak (50MWS) Project has created a dynamic networking Digital Platform for African women entrepreneurs. The Platform will enable women to connect with one another in ways that will foster peer-to-peer learning, knowledge exchange/transfer, mentoring and the sharing of information and knowledge within communities, and provide them with access to trade finance and market opportunities between urban and rural areas, and across borders and between countries. In addition, the Platform will enable women to develop market intelligence skills to stay abreast of business development trends within their contexts, regionally and globally to ensure sustainability of their businesses. The project is implemented in 38 countries belonging to COMESA, EAC and ECOWAS

II. Why risk assessment

As the world gets more connected, and everyone migrating to online services, the security of information is becoming more important to everyone. The year 2016 marked the entrance of a new wave of threats and vulnerability that have changed the cybersecurity landscape. This year all organizations continue to face cyber-attacks of different kind and magnitude. The COMESA, EAC and ECOWAS did not ignore these facts, the mentioned RECs would like to create a culture of protection and increase its technical capabilities to detect and eliminate potential cyber threats.

Looking at how COMESA,EAC and ECOWAS are interconnected from an information technology perspective (platform), and again the value of the information that its systems hold and generate, it's time to ensure that we have sound strategies that will allow our institutions to manage their IT assets and protect them from any kind of attack. It is in this regard that the COMESA, EAC

and ECOWAS would like to conduct a quick risk assessment for the mentioned platform.

By definition the risk assessment is defined as the process of identifying variables that have the potential to negatively impact an organization's ability to conduct business. When it comes to information technology security, information security risk assessment is an on-going process of discovering, correcting and preventing security problems. The risk assessment is an integral part of a risk management process designed to provide appropriate levels of security for information systems. The risk assessment is one of the key components of every security program. Conducting a risk assessment is not only a best practice but it's a mandatory practice that RECs would like to enforce internally. The end result of this risk assessment will be a report which contains the following:

- Summarizes the system architecture and components, and its overall level of security
- Includes a list of threats and vulnerabilities, the system's current security controls, and its risk levels
- Recommends safeguards, and describes the expected level of risk that would remain if these safeguards were put in place
- Shows where the project needs to concentrate its remedial work
- In-depth analysis/resolution of specific security incidents or violations
- List of recommended changes (policies, standard compliance and practical), with approximate levels of effort for each

III. Scope - The work to be conducted by the consultant

The consultant will conduct a cyber security audit and conduct Risk Assessment for infrastructure and system hosted in COMESA Head office in Lusaka, Zambia and Microsoft Azure cloud.

The consultant is expected to deliver an Information Security Risk Assessment Report and a Cyber Security Audit report. The next sections describe in details the expected work to be conducted:

a. The consultant is required to conduct tests and analysis of platform technical environments for sound architectures, correct configurations, and system-level vulnerabilities.
b. The information security risk assessment report will contain both high-level and detailed information about the assessment.

c. The Cyber Security audit report that will be developed by the consultant will provide a blueprint to 50 million Africa women speak project's(50MAWSP) leadership which builds upon the information learned during the assessment and will give project's a strategy for achieving a high level of security program maturity in the shortest time frame possible.
d. The consultant should help the leadership to understand key risks by assigning each risk profile component a component risk score. These scores should cover the following core security program components:
    - Regulatory Compliance and Information Security Policy
    - Processes and Procedures
    - Technical Architectures and Configurations
    - Vulnerability and Patch Management
    - Security Controls and Continuous Monitoring
    - Threat Detection and Incident Response
    - Resources, Skills and Awareness Training
e. The consultant should run a seminar/workshop with Project key technical staff in order to share current industry best practices in cyber security and the findings of the information security risk assessment**.**
f. The consultant will also run a half day executive cyber security awareness program with the senior management/project management team and will discuss findings of the enterprise risk assessment.

IV. Duration of the assignments:

The assignment is expected to be carried out over a period of 45 days.

V. The consultant – Expected profile

This consultancy is open to consulting firms that have the following profile;

a. At least 10 years of industry experience in the cyber security domain.
b. The consulting firm should be able to have at least 3 similar completed projects recently.
c. Wealth of experience supporting diversified international clients (governments, non-governmental organizations and private sector)
d. Staff qualifications in cyber security, penetration testing and familiarity with industry best practice frameworks as outlined below:
    - Certified Ethical Hacker
    - Certified CNO Tooling Professional
    - Offensive Security Certified Professional

- Defensive Security Certified Professional
- Certified Penetration Testing Professional
- Certified professional developer, Java, PHP, MySQL, Oracle, PostgreSQL and other Opensource Technologies
- Certified professional Networking virtualization storage, cloud technologies
- Certified ISO/IEC 27001 Lead Implementer
- Certified ISO/IEC 27001 Lead Auditor
- CISA
- CISP will be added advantage

VI. Project Deliverables

a. Inception report: To be developed within 2 Weeks of commencing the assignment.
b. Bi-weekly progress report: To be submitted every two weeks, this report should contain what has been completed during the closing period, challenges and planned work in the next period.
c. Information Security Risk Assessment Report and Cyber Security audit report.
d. A meeting with technical/non-technical staff covering current industry best practices in cyber security and the findings of the Information Security Risk Assessment**.**
e. A half day executive cyber security awareness seminar with the senior management.
f. Project closeout executive presentation on the key findings from the risk assessment and lead a conclusive discussion on the cyber security audit report.