pasgr.org
PARTNERSHIP FOR AFRICAN SOCIAL
& GOVERNANCE RESEARCH

Date: May 19, 2023

Terms of Reference - Information Systems Audit and Policy Review

Background

The Partnership for African Social and Governance Research (PASGR) is an independent, non-partisan, pan-African not-for-profit organisation established in 2011 and located in Nairobi, Kenya. Currently engaged in more than 26 African countries, PASGR works to enhance research excellence in governance and public policy that contributes to the overall wellbeing of women and men. In partnership with individual academics and researchers, higher education institutions, research think tanks, civil society organisations, business, and policy communities both in the region and internationally, PASGR supports the production and dissemination of policy relevant research; designs and delivers suites of short professional development courses for researchers and policy actors; and facilitates the development of collaborative higher education programmes.

PASGR's information technology systems comprise of:

- a Local Area Network (LAN) - cabled and wireless as well as Virtual LANs
- a cloud infrastructure with applications and websites, and
- an entire Office365

LAN hardware includes servers running Microsoft Windows Server operating systems (OS), Windows and Mackintosh OS workstations, and multivendor networking devices. Core ERP is a Microsoft system. The organization has several cloud-based applications including websites which are hosted by outsourced technology service providers.

PASGR intends to carry out an Information Systems (IS) Audit that will evaluate and determine security and policy decisions required to ensure protection of all internal information resources. PASGR therefore invites Expressions of Interest (EoI) from consultants/consulting firms having a minimum of seven years' experience and a proven track record in projects of similar nature, who wish to carry out the IS Audit exercise.

The IS Audit will entail conducting a risk assessment of the IS Systems at PASGR offices, identification, and evaluation of the risks. In the light of the risk assessment exercise, the selected consultants/consulting firms should recommend and assist in implementing a set of best practices governing the Management of Information Systems within the organisation.

The duration of the IS Audit exercise is expected to be 7 working days. The consultants/consulting firms should deliver at the end of the Audit exercise, a complete Audit Report comprising an Executive Summary, Findings and Recommendations which should include current systems vulnerabilities, and detailed technical implementation roadmap to address any identified gaps.

Objectives

The consultants/consulting firm will review current policies last reviewed in 2014, conduct IT audit and obtain reasonable assurance that the internal control measures in place provide the required level of information security to ensure availability, confidentiality, and integrity of PASGR's information systems including the financial applications (Gap analysis). This includes but are not limited to:

a) Review PASGR's information security risk management controls and policies to secure organisation's data against risks.
b) Obtain reasonable assurance that the information systems are reliable and meet ISO27001 -2022 information security standards.
c) Review PASGR's Information systems architecture to evaluate both logical and physical security of the organisation's information assets.
d) Evaluate PASGR's measures in place for Business Continuity and the ability to recover organisation's data in case of a disaster.
e) Evaluate security of organisational data stored both locally and offsite, with special focus on finance, project data and Office365 platform.

Scope - Information Systems (IS) Audit

A comprehensive Information Systems Security Audit must be undertaken covering the various key processes and procedures undertaken at PASGR offices in the two areas namely:

a) PASGR local IT Infrastructure
b) PASGR cloud / off-site IT Infrastructure including Office365.

A complete audit of the systems shall be completed within seven working days from the agreed start date once a contract is signed.

This IS/IT Audit shall include, but not be limited, to the following: -

1) Operating System (OS) for servers, databases, network equipment, security systems, storage area networks.

i. Set up and maintenance of system parameters.
ii. Patch Management
iii. Change Management Procedures
iv. Logical Access Controls
v. User Management & Security

vi. Operating System Hardening
vii. Performance, Scalability and Availability

2) Review of IT Processes and IT Management Tools

i. IT Assets Management
ii. Financial Management System
iii. IT Support
iv. Change Management
v. Incident Management
vi. Network Management
vii. Backup & Media Management
viii. Anti-Virus Management
ix. Vendor & SLA Management

3) Security Management

i. Security Equipment Configurations & Policies
ii. Penetration testing and Vulnerability Assessment (PT / VA) of various security zones.

4) Network & systems audit

i. Network architecture review
ii. Network traffic analysis and base lining
iii. Wireless LANS and VLANs

5) Review the PASGR's policy document and all IT policies

Review for currency and improvement of existing policies and recommend removal of any redundant/ineffective policy as well as inclusion of any missing compliance policy in line with best practice and in consultation with PASGR.

6) Software and Applications Review

Audit computer software and applications in use at PASGR and provide recommendations on effectiveness, security, versions etc.

7) Business Continuity

Review and evaluate PASGR's Disaster Recovery Plan.

8) IT Staffing

Evaluate PASGR's Information technology needs and provide recommendations on IT staffing.

9) Hardware and the IT Infrastructure

Audit current hardware, devices, and technical infrastructure for relevance and applicability.

10) Others

Audit all other areas as comprised in the current PASGR IT policy document with special focus on emerging areas.

Deliverables

a) Inception Report (proof of understanding of the assignment and audit implementation plan)
b) IT audit report
c) Draft revised PASGR IT Policy document.
d) PASGR costed implementation plan.
e) Outline of key tools; open source or proprietary for target applications and systems to aid in automated efficient execution of PASGR IT processes.
f) Final PASGR IT Policy document

Skills and Qualifications

The Service Provider consultant(s) must have knowledge and experience in the following areas:

a) No less than 10 years of demonstrable experience in designing IT Policies/ strategies and implementation plan for donor-funded organisations. Experience in ICT governance at the regional level or with entities of similar nature across Africa would be an added advantage.
b) Have technical capacity to undertake the task including but not limited to a competent and diverse project team that is able to revise, design, deploy and plan tools, procedures, guidelines, standards, policies from a best practice perspective as may be agreed with PASGR.
c) Have demonstrated experience of not less than 7 years' experience in working across ICT, commerce, or audit firms.
d) At least a Master level degree in either Computer Engineering, Telecommunications Engineering, Software Engineering, Computer Science, Information Technology, and Information Systems Management with especially demonstrable experience in information systems security. Global certifications in areas of CISSP, CISO, CISM, CEH, Security+ or equivalent will be an added advantage.
e) Excellent communication skills, both orally and in writing, and fluency in written and spoken English is mandatory.

Requirements

a) Expressions of Interest shall include the qualifications and experience of the consultants expected to work on the project.
b) Details of similar projects carried out by the consultants/consulting firms should be included.

c) PASGR reserves the right to accept or reject any expression of interest and to annul the exercise and reject all expressions of interest without thereby incurring any liability to any participant or any obligation to inform those who have expressed interest of the grounds of its action.

d) The selected consultants/consulting firm shall be required to make a detailed presentation of the IS Audit exercise.

e) Expressions of interest received after the date and time stated below shall not be considered.

Response to the ToR.

The EOI proposal should cover:

- Your understanding of the assignment
- Evidence of past work experience
- A proposed approach and methodology for carrying out the assignment.
- Core team, responsibilities, and level of effort.
- A detailed work plan, timeframes, milestones, and budget.

Please respond to this EOI with not more than 10 pages of technical and financial proposal (including all the attachments) to **it@pasgr.org** by 5:00 p.m. EAT Friday June 23, 2023.