TERMS OF REFERENCE AND SCOPE OF SERVICES FOR THE POSITION OF INFORMATION SYSTEM SECURITY RISK ANALYST - HUMAN CAPITAL MANAGEMENT/MINISTRY OF PUBLIC SERVICE

Background

The Ministry of Public Service has been implementing the Integrated Personnel and Payroll System (IPPS), a computer based Human Resource Information System that manages the processing and payment of Government of Uganda Salaries, Pension and Gratuities. IPPS also facilitates the establishment control and management of the Public Service Organisations.

Government of Uganda is in the process of procuring a Human Capital Management (HCM) system that will seamlessly integrate with Integrated Financial Management System and other Government ICT systems but also automate all Human Resource functions across Government Ministries, Departments, Agencies and Local Governments.

To achieve successful implementation and deployment of the HCM system, the Ministry of Public Service seeks to recruit highly motivated personnel to provide technical support to the HCM project. The recruited personnel will be required during the Pre and Post Project Implementation Period.

Objective:

To provide project risk management support to Ministry of Public Service (MoPS) in areas of information system security analysis, evaluating the risk exposure, identifying risks, planning and developing suitable responses to mitigate or avert possible risks and/or threats to the implementation of the new Human Capital Management System project.

Specific Duties and Responsibilities:

The Risk Analyst will be required to perform the following duties and responsibilities:

i Evaluate and review internal controls of the existing information systems and related ICT infrastructure and advise on the information system security to guide transition to the new HCM.

ii Develop and monitor implementation of information security policies, procedures, controls and technical systems in order to maintain the confidentiality, integrity, and availability of the HCM system.

iii Perform information security risk assessments to ensure appropriate information security and business continuity controls exist including identifying, describing, analysing and estimating the risks.

iv Identify and evaluate technology risks, mitigating controls, and opportunities for control improvement.

v Establish Standard Operating Procedures (SOPs)/criteria for proper management of HCM risks.

vi Provide technical support in organizational risk reporting across project strategic, tactical and operational levels and across key stakeholders.
vii Build staff capacity in risk awareness, analysis and management.
viii Monitor systems, identify and report violations of risk limits/controls.
ix Evaluate the effectiveness of organizational controls, perform risk analysis and management activities and develop appropriate mitigation plans.
x Identify necessary enhancements for organizational business processes and policies to prevent operational project risks.
xi Undertake audits of organizational policies relating the HCM project and ensure compliance with National standards, legislations and frameworks.
xii Conduct self-assessments of the HCM information security management system to ensure the effective implementation of and compliance with the National Information Security Framework.
xiii Develop and maintain an up-to-date risk register for the HCM.
xiv Review and enhance existing risk modelling techniques.
xv Perform procedures and assessments necessary to ensure the safety of information assets.
xvi Undertake continuous risk based system audits in accordance with the annual work plans.
xvii Conduct operational, compliance and investigative assessments.
xviii Ensure that a complete and cross referenced audit engagement plan is maintained for every audit engagement.
xix Monitor the HCM and supporting infrastructure through adequate audit logging, scanning, and monitoring processes.
xx Provide risk and control advisory to the Ministry on pre and post implementation system development and enhancements.
xxi Conduct general and application control reviews for computer information systems and databases in respect to development standards, operating procedures, system security, programming controls, communication controls, backup and disaster recovery, and system maintenance.
xxii Monitor the resolution of all incidents and incident handling and escalation procedures to ensure effective incident resolution.
xxiii Champion data mining and analytics use and capability development within the team.
xxiv Monitor developments in ICT risk management and audit approaches in the industry, assess viability and recommend actions for implementation and improvement.
xxv Any other duties as may be assigned from time to time.

Qualifications and Experience

1. Bachelor’s degree in Computer Science, Information Technology, Information Science, Information Systems, Information Security or a related field from a recognized university.
2. A professional qualification in IT Industry Certifications such as CRISC, CISA, CISM, CISSP, ISO 27001 or ISO 31000.
3. Possession of PMP, Prince2, of ITIL will be an added advantage.

4. Four (4) years working experience in Risk Management or Information Security Management Information Systems Audit or ICT Audit consulting or a related field with Two (2) years at a supervisory level.
5. Experience in Governance Risk and Compliance tools as well as mechanisms.
6. Experience in Oracle databases, networks and systems management and implementation of ICT projects.

Knowledge, Skills, and Abilities Required

i Working knowledge of National information risk management frameworks and standards.

ii Broad knowledge of Information System Security.

iii Demonstrable interest in information security and IT audit developments.

iv Knowledge of Risk Management.

v Analytical and problem solving skills.

vi Good Communication & interpersonal skill across strategic, tactical and operational levels.

vii Stakeholder Management skill.

viii Flexibility, persistence and willingness to work on a variety of activities/tasks.

ix Logical and objective attention to detail, analytical abilities and the ability to recognize trends in data.

x A proactive approach with the confidence to make decisions.

xi A methodical and well-organized approach to work.

xii The ability to work under pressure and meet deadlines.

xiii Confidentiality of Government information.

xiv Knowledge of Government procedure, processes and operations.

Outputs

1. Evaluation report on system security and internal controls of the existing information systems and related ICT infrastructure.
2. Guidelines on the required information system security to support transition to the new HCM.
3. Information system security and controls policy developed.
4. Audit engagement plan developed and maintained for every audit engagement.
5. Information System security audit reports provided quarterly.
6. Documentation and dissemination of Standard Operating Procedures (SOPs)
7. Strategy and plan for staff capacity building in risk awareness, analysis and management developed.
8. Risk management strategy for HCM developed and an up-to-date risk register maintained.
9. Quarterly and Annual Performance reports.

Reporting Arrangement

The Information System Security Risk Analyst will report to the Project Manager/IPPS and will provide monthly, quarterly and annual performance reports.

Contract Arrangements

The assignment is for one (1) year and may be renewed based on need and satisfactory performance.

Facilities to be provided by the Client

Ministry of Public Service will make available on request all data necessary in carrying out the assignment. Ministry of Public Service will also provide office space and relevant office facilities during the period of the assignment.