TERMS OF REFERENCE AND SCOPE OF SERVICES FOR THE POSITION OF INFORMATION SYSTEM SECURITY RISK ANALYST

MINISTRY OF PUBLIC SERVICE

1.0. Background

The Ministry of Public Service is 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. Currently, the IPPS environment presented risks which pose challenge to its survival and existence to effectively achieve the intended reform purpose.

To address some of the challenges, Government of Uganda has decided to procure a Human Capital Management (HCM) system that will seamlessly integrate with Integrated Financial Management System and other Government ICT systems and facilitate the automation of all Human Resource functions across Government Ministries, Departments, Agencies and Local Governments. The transition of IPPS' underlying software application to the Human Capital Management application and change of host environment to the National Data centre is envisaged to present a yet more of technological, operational, Fraud, compliance and governance challenges which must be closely monitored and managed.

To this effect, the Ministry of Public Service has identified the need for strengthening its internal capacity and seeks to recruit a highly motivated personnel to provide technical support in security and risk management of the IPPS environment.

2.0. Objective

To provide technical expertise to ensure the Integrated Personnel and Payroll System infrastructure, applications and information assets are protected. The Information System Security Risk Analyst will develop and drive security strategies, policies/standards, ensuring the effectiveness of solutions, and provide security-focused advisory services to the Ministry of Public service.

3.0. Specific Duties and Responsibilities:

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

1. Develop, refine, maintain and implement enterprise-wide Information Security and Risk policies, procedures and standards to meet compliance responsibilities.
2. Develop and implement strategies to align information security with MOPS business objectives and goals, protecting the integrity, confidentiality and availability of data on the IPPS existing software application in preparation for transition to the HCM.
3. Work directly with the IPPS users, third parties and other internal departments to facilitate information security risk analysis and risk management processes to identify acceptable levels of residual risk.

4. Assess information security alerts, threats and vulnerabilities to the IPPS/HCM environment, recommend and manage the appropriate security controls & measures for information systems.
5. Conduct detailed risk assessments and baseline control analysis, and provide actionable recommendations.
6. Conduct business impact analysis to ensure that key resources both tangible and intangible are adequately protected with proper security measures and controls.
7. Participate in cost-benefit and risk analysis.
8. Manage the update and maintenance of an enterprise risk framework (a single view of the risk profiles and tolerance.)
9. Evaluate security risks, identify and define compliance strategies in accordance with policies, standards, guidelines and procedures.
10. Monitor systems, identify and report residual risks, vulnerabilities, security exposures, security violations and violations of risk limits/controls, including misuse of information assets and noncompliance.
11. Provide support in security incident and response management and assist in troubleshooting, identification of root causes and resolving security related issues and problems.
12. Maintain risk management procedures, Institution continuity scenarios, and contingencies and advise on Institution continuity and disaster recovery plans.
13. Participate in designated projects such as HCM, developments or business initiatives, advising on information security risks through the project life cycle.;
14. Undertake continuous risk based system audits in accordance with the annual work plans and provide support to business during internal or external audit sessions, including Penetration Tests & Ethical hacks;
15. Provide technical support and guidance in the review and implementation of change requests.
16. Generate appropriate communication, process and educational plans for mitigating the disruption of change in accordance with the MOPS IT Change management policy.
17. Develop, deliver IT risk & security awareness and compliance training programs and. build staff capacity in risk awareness, analysis and management.
18. Any other duties as may be assigned from time to time.

4.0. 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/ ISO 31000 is required.
3. Possession of PMP, PRINCE2, and/or ITIL will be an added advantage.
4. Four (4) years working experience in Risk Management or Information Security, Management of Information Systems Audit or ICT Audit consulting or a related Information Security field with two (2) years at a supervisory level in IT Security.
5. Demonstrable experience of using Risk Management and Security frameworks.
6. Experience in designing and implementing security solutions, Governance, Risk and Compliance tools as well as mechanisms.
7. Demonstrable experience in Information System Security techniques, with a broad range of exposure to systems analysis, application development, systems administration

8. Experience in relational databases such as Oracle, networks and systems management and implementation of ICT projects.

5.0. Knowledge, Skills, and Abilities Required

1. Knowledge of National information risk management frameworks and standards.
2. Knowledge of information security industry trends.
3. Good Communication & interpersonal skill across strategic, tactical and operational levels.
4. Stakeholder Management skills.
5. Flexibility, persistence and willingness to work on a variety of activities/tasks and work under pressure.
6. Logical and objective attention to detail, analytical abilities and the ability to recognize trends in data.
7. A proactive, methodical and well-organized approach to work with the confidence to make decisions.
8. Confidentiality of Government information.

6.0. Outputs

1. Enterprise-wide security policies, procedures, baselines and Standard Operating Procedures (SOPs) to meet compliance responsibilities developed.
2. Enterprise-wide security policies, procedures Standard Operating Procedures (SOPs) for security and risk management disseminated and implemented.
3. Evaluation report on system security and internal controls of the existing information systems and related ICT infrastructure.
4. Guidelines on the required information system security controls and remedial actions to support transition to the HCM.
5. Audit engagement plan developed and maintained for every audit engagement.
6. Information System security audit reports provided quarterly.
7. Strategy and plan for staff capacity building in information security and risk awareness, analysis and management developed.
8. Enterprise Risk management strategy developed
9. Comprehensive risk register maintained.
10. Quarterly and annual reports on Compliance with security policies, standards, guidelines and procedures.
11. Quarterly and Annual Performance reports on the effectiveness of information security and adoption of new policies and procedures
12. Quarterly evaluations of security controls, mechanisms and goals in comparison to best practices.
13. Disaster recovery test plans for IPPS/HCM.
14. Periodic Business Continuity and Data Recovery test drill reports.
15. Implementation plans for activities related to compliance, control assurance, risk management, security, and infrastructure/information asset protection.

7.0. Reporting Arrangement

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

8.0. Contract Arrangements

The assignment is for one (01) year and may be renewed based on need and satisfactory performance.