Job Description

9th Floor Tanzanite Park, Victoria, Dar es Salaam, Tanzania | +255 758 778 886 | info@empower.co.tz

Job Title
Security and Governance Specialist

Job Location
Dar es Salaam

Category
-

Job Type
Full Time

Job level
Intermediate

Industry
Entertainment

Open to Expatriates
Only Open to Tanzanian Nationals

Minimum Requirements

Min Budget
-

Max Budget
-

Primary Industry
Entertainment: 10 Years

Secondary Industry
-

Primary Category
-

Secondary Category
-

Certificate
-

Qualification
-

Summary

This role involves steering the conceptualization and implementation of all IT GRC and Security architecture. Taking ownership of all direction, vision, standards and strategic objectives for security architecture as well as all IT Governance and compliance.

Responsibilities

- Work closely with data governance and internal audit/risk teams to define the systems access levels for different roles in the organization
- Work closely with Human Resources to ensure that employees who exit the organization have their access revoked on their last day in the office. Regularly obtain exit reports and cross check to ensure that the user access has been removed
- Measure and report to management on the progress of data quality improvement Define and establish an IT governance framework in line with the corporate governance
- Define and communicate an IT governance maturity roadmap
- Monitor and report on IT governance initiatives
- Prepare reports on IT strategy, performance and risks
- Assess the IT infrastructure on a periodic basis to ensure that it is standardized wherever possible
- Oversee the development and implementation of information security standards for all part of the lottery division – lotto specific data and information as well as generic systems such as accounting and payroll systems
- Undertake period reviews of the information security strategy, procedures, policies standards and guidelines to keep up with the prevailing best practices
- Define and implement the standards for logical access management including user ID creation, password/authentication standards, monitoring and access lock-down
- Conduct information security related investigations, monitor and report to ensure conformity to the set IT standards
- Monitor adherence to information security standards by conducting monthly dipstick audits Commission formal external audit reviews (such as testing for hacking/unauthorized access) once approval for these activities is obtained from the Chief Operating Officer
- Drive the creation of awareness communication materials as well as more in-depth training for employees on information security
- Review requests for whitelisted websites and email addresses and assess whether they meet the standards to be included. Authorize the firewall changes
- Participate in the creation of standards to ensure the separation of duties to ensure protection against collusion and processing of incorrect or fraudulent transactions
- Participate in the creation of policies and process for the destruction of data or removal of confidential information from hardware used in the organization. Ensure that the correct hardware and software applications are in use to protect

confidential information from accidentally being recovered from unused equipment
- Deploy software and tools to monitor the appropriate use of data and information. Highlight breaches including the severity of the breaches. Work with Human Resources to run disciplinary processes to address the breaches
- Be accountable for the design and deployment of appropriate processes, tools and technologies
- Ensure that Security Management is engaged with regards to service assurance
- Ensure compliance with its regulatory obligations in regards to IT assets, where operational processes depend on IT performance, keeping abreast of regulations on third party risk, maintaining external networks for the purpose of identifying best practice
- Lead the completion of Service Introduction Assessments
- Create and manage a risk governance framework
- Provide monthly and quarterly reports on implementation of initiatives for accountability and performance monitoring

Education & Qualifications

- Bachelors degree in Commerce or Law and IT
- CISA, CISM, CISSP or equivalent IT governance and risk management certifications
- Post graduate qualification in law enforcement, forensics or information security management

Requirements

- A minimum of 10 years experience in security and IT security, IT Risk and IT Audit field

Reporting To

IT Manager

Driving Licence

Not Required

To Apply for This Job Click Here