GENERAL:

Job Title: Senior Officer, Internal Audit, Information Systems Audit
Department: Internal Audit
Job Grade: Senior Officer
Reports to: Manager, Internal Audit, Information Systems Audit

No. of Vacancies: 1

JOB PURPOSE:

The Senior Officer, Internal Audit, Information Systems Audit, will perform Information Systems audit procedures, including testing, evaluating, and improving the effectiveness of IT controls, cybersecurity measures, and governance processes. This role involves participating in the planning, execution, and reporting of IT audit engagements, covering business and support operations, applications, infrastructure, networks, and third-party services. The officer will also follow up to ensure that IT audit recommendations, management corrective actions, and Board directives are effectively implemented.

MAIN DUTIES AND RESPONSIBILITIES:

- Support the Assistant Manager or Manager, IS Audit, in conducting IT risk assessments and defining the objectives, scope, and methodology for IT and cybersecurity audit engagements and the annual audit plan.
- Execute IT audit assignments covering applications, databases, operating systems, networks, cybersecurity, cloud, and third-party services, in line with the approved audit plan and professional standards.
- Evaluate the adequacy and effectiveness of IT controls, cybersecurity measures, data protection, and governance processes.
- Perform detailed control testing to assess general IT controls, application controls, and system configurations for compliance with policies, procedures, and regulatory requirements.
- Conduct reviews of ICT operations, system changes, and project management practices to assess risk management and control adequacy.
- Use data analytics and automated audit tools to identify anomalies, trends, and indicators of control weaknesses or potential fraud.
- Participate in cybersecurity reviews, vulnerability assessments, and incident management audits to assess resilience and response effectiveness.
- Review compliance with ICT, cybersecurity, and data privacy policies, including regulatory requirements related to information security and data governance.
- Contribute to the preparation of IT audit reports, summarizing key observations, control deficiencies, and actionable recommendations.
- Follow up on implementation of IT audit recommendations to ensure timely and effective remediation of identified issues.
- Participate in ad hoc and special reviews, including forensic, cybersecurity, or system integrity investigations, as requested by management or the Audit Committee.
- Support the use of computer-assisted audit techniques and continuous auditing methods to enhance audit coverage and efficiency.
- Stay abreast of emerging IT risks, technologies, and cyber threats to support the development of data-driven, risk-based audit approaches.
- Ensure all work aligns with the Internal Audit Policy, International Professional Practices Framework (IPPF), and ISACA standards.
- Perform any other duties assigned by the Assistant Manager, Manager, or Head of Internal Audit.

QUALIFICATION, SKILLS AND KNOWLEDGE:

QUALIFICATIONS:

- Bachelor's degree in Information Technology, Computer Science, Information Systems, or a related field from a recognized higher learning institution.
- Professional certification such as CISA, CISM, CRISC, CEH, or CIA will be an added advantage.

SKILLS, KNOWLEDGE AND ATTRIBUTES:

- Comprehensive understanding of IT governance, information security, IT general and application controls, and frameworks (e.g., ISO 27001, NIST, PCI-DSS, COBIT).
- Strong analytical and problem-solving skills, with an investigative and skeptical mindset.
- Proficiency in the use of data analytics tools (e.g., ACL, IDEA, SQL, Power BI) and audit management applications (e.g., TeamMate).
- Good understanding of networking, databases, operating systems, and cloud environments from a control and audit perspective.
- Excellent written and verbal communication skills, with the ability to present technical issues clearly to both technical and non-technical audiences.
- Ability to work effectively under tight deadlines, manage multiple audit assignments, and deliver high-quality results.
- Demonstrated integrity, sound judgment, and attention to detail in performing audit tasks.

EXPERIENCE

- At least two (2) years of experience in IT auditing, cybersecurity assessment, or technology risk management, preferably in a banking or financial institution environment.

If you believe you can clearly demonstrate your abilities to meet the criteria given above, please submit your job application cover letter along with a detailed resume, copies of the relevant certificates and testimonials in a single PDF file format, quoting the respective Job title or Ref no. in the subject field to **TZRecruitment@equitybank.co.tz** by **Tuesday 29th November 2025**

Only short-listed candidates will be contacted.

Equity Bank is an equal opportunity employer. We value the diversity of individuals, ideas, perspectives, insights and values, and what they bring to the workplace.

By submitting your application, you consent to Equity Bank Tanzania Limited collecting and processing your personal data strictly for recruitment, selection, and, where applicable, employment purposes. Equity Bank Tanzania Limited will process your personal data in accordance with the Data Protection and Privacy Act, Cap 97, and its Data Privacy Policy. Your personal information will be treated with the highest level of confidentiality and will not be shared with unauthorized third parties, except where disclosure is required by law or regulatory obligation".