Job Ref. No: JLIL373

Position: Information Systems Auditor

Jubilee Insurance was established in August 1937, as the first locally incorporated Insurance Company based in Mombasa. Jubilee Insurance has spread its sphere of influence throughout the region to become the largest Composite insurer in East Africa, handling Life, Pensions, Asset Management and Medical Insurance. Today, Jubilee is the number one insurer in East Africa with over 1.9 million clients. Jubilee Insurance has a network of offices in Kenya, Uganda, Tanzania, Burundi. It is the only ISO certified insurance group listed on the three East Africa stock exchanges – The Nairobi Securities Exchange (NSE), Dar es Salaam Stock Exchange and Uganda Securities Exchange. Its regional offices are highly rated on leadership, quality and risk management and have been awarded an AA- in Kenya and Uganda, and an A+ in Tanzania. For more information, visit www.JubileeInsurance.com.

We currently have an exciting career opportunity for an **Information Systems Auditor** within **Jubilee Life Insurance Limited.** The position holder will report to the **Group Head of Internal Audit** and will be based at our Head Office in Nairobi.

Role Purpose

The Information Systems Auditor is responsible for executing IT and internal audit assignments across Jubilee Insurance and, where necessary, regional entities. The role evaluates IT controls, cybersecurity practices, information system processes, and technology-enabled business operations to determine whether controls are effective and risks are adequately mitigated. The auditor provides independent assurance to Management and the Audit Committee and supports strengthening of the Company's governance, risk, and control environment.

Key Responsibilities

Strategy

1. Provide insights and analysis to support strategic decision-making related to IT risk management, cybersecurity, and internal controls.
2. Identify opportunities to optimize technology-enabled processes and improve the efficiency of IT controls.
3. Assess IT governance practices and recommend enhancements aligned with industry standards and regulatory requirements.
4. Evaluate performance of IT functions and provide feedback to improve strategic alignment and operational effectiveness.

Operational

1. **Plan and Execute IT Audits:**

- Develop risk-based IT audit plans and programs.
- Conduct fieldwork, gather evidence, and document audit findings.

- Evaluate IT general controls (ITGC), application controls, cybersecurity controls, and infrastructure security.

2. **IT Risk Assessment:**
- Identify risks in IT systems, networks, applications, and technology-enabled processes.
- Assess potential impacts on data integrity, financial reporting, operations, and compliance.
- Recommend risk mitigation measures to relevant stakeholders.

3. **Compliance & Regulatory Review:**
- Ensure compliance with IT laws, cybersecurity regulations, and industry standards.
- Monitor changes in IT and cybersecurity requirements and assess their impact.
- Advise management on technology-related compliance risks.

4. **Financial & System Data Analysis:**
- Review system-generated financial data and transaction trails for accuracy and completeness.
- Identify anomalies, irregularities, and potential internal control weaknesses.

5. **Process Improvement:**
- Recommend enhancements to IT processes, system controls, and internal procedures.
- Support continuous improvement initiatives to strengthen the control environment.

Corporate Governance
1. Ensure all audit assignments comply with internal audit standards, Company policies, and regulatory requirements.
2. Promote strong IT governance, cybersecurity awareness, and internal control culture across business units.
3. Prepare and submit IT audit reports, findings, and recommendations to Management and the Audit Committee.
4. Ensure adherence to IT governance and cybersecurity frameworks such as ISO 27001, ISO 22301, COBIT, and NIST.

People and Culture
1. Provide training and guidance to staff on IT controls, cybersecurity practices, and risk awareness.
2. Foster a culture of accountability, confidentiality, and integrity across the Company.
3. Collaborate with IT, Risk, Compliance, and business teams to ensure timely follow-up and closure of audit recommendations.
4. Support capability development within the Internal Audit function through sharing of knowledge and expertise.

Key Competencies
1. Strong understanding of IT systems and infrastructure.
2. Good knowledge of cybersecurity principles and practices.
3. Analytical and critical-thinking abilities.
4. High attention to detail and precision.
5. Effective communication and audit report-writing skills.
6. Teamwork and stakeholder management.
7. Confidentiality, ethical conduct, and professionalism.
8. Strong planning and organizational skills.

Functional Skills

1. Knowledge of IT audit methodologies, internal audit standards, and risk-based auditing.
2. Ability to identify IT and cybersecurity risks and recommend effective mitigation strategies.
3. Strong financial and data analysis capabilities.
4. Understanding of IT compliance requirements and regulations.
5. Familiarity with process improvement methodologies (e.g., Lean, Six Sigma).
6. Proficiency in audit software and analytics tools.
7. Knowledge of IT governance and security frameworks such as ISO 27001, ISO 22301, COBIT, and NIST.

Key Deliverables for the Role

1. Risk-based IT and internal audit plans and programs.
2. Comprehensive audit working papers and evidence documentation.
3. High-quality audit reports highlighting findings, risks, and recommendations.
4. IT risk assessments and compliance evaluation reports.
5. Follow-up reports on remediation of IT control weaknesses.
6. KPI dashboards for audit execution, findings, and issue tracking.
7. Positive stakeholder feedback and value-add through audit insights.

Academic Qualifications

1. Bachelor's degree in Computer Science, Information Systems, IT, or a related field.
2. Certifications such as CISA, CEH, CISSP, CISM, CGEIT, or CRISC are an added advantage.
3. Training in RPA, Machine Learning, or Data Analytics is an added advantage.

Relevant Experience

1. Minimum four (4) years of experience in IT audit, information systems audit, cybersecurity audit, internal audit, or related fields.
2. Experience in software development, IT operations, or Big 4 consulting is an added advantage.
3. Demonstrated experience evaluating, designing, and implementing IT controls.
4. Experience conducting system-based audits and compliance reviews.
5. Evidence of participating in control design, development, and monitoring activities.

If you are qualified and seeking an exciting new challenge, please apply via Recruitment@jubileekenya.com quoting the Job Reference Number and Position by 18th January 2026

Only shortlisted candidates will be contacted.