UBA
United Bank for Africa

JOB ADVERT

About UBA

United Bank for Africa (UBA) is one of Africa's leading financial institutions, with operations in twenty (20) countries and four (4) global financial centers: London, Paris, Dubai and New York. UBA has evolved into a Pan-African, provider of banking and related financial services through diverse channels globally.

United Bank for Africa Uganda represents UBA's pioneer country activities in the East and Southern African sub-region. With a growing network of branches and ATMs across the country, the bank continues to expand the retail and commercial playing field in Uganda by delivering unique financial products and solutions. The bank is seeking to recruit the following highly motivated, competent, result oriented and dynamic professionals for the following positions;

JOB TITLE: **CHIEF INFORMATION SECURITY OFFICER**
REPORTS TO: **GROUP CISO & COUNTRY CEO**

ROLES & RESPONSIBILITIES

1. Establish Governance & Build Knowledge

- Facilitate an information security governance structure within Country/Region through the implementation of a hierarchical governance program
- Provides regular reporting on the current status of the information security program to enterprise risk teams and senior business leaders as part of a strategic enterprise risk management program, thus supporting business outcomes
- Develops, socializes and coordinates approval and implementation of security policies within Country/Region
- Works with the vendor management office to ensure that information security requirements are included in contracts by liaising with vendor management and procurement organizations
- Directs the creation of a targeted information security awareness training program for all employees, contractors, and approved system users, and establishes metrics to measure the effectiveness of this security training program for the different audiences
- Understands and interacts with related disciplines, either directly or through committees, to ensure the consistent application of policies and standards across all technology projects, systems and services, including privacy, risk management, compliance and business continuity management
- Provides clear risk mitigating directives for projects with components in IT, including the mandatory application of controls
- Embeds Cyber Judgement across a decentralized or distributed decision making model
  Leads the security champion program to mobilize employees in all locations

2. Leadership

- Leads the information security function within the Country/Region to ensure consistent and high-quality information security management in support of the business goals
- Determines the information security approach and operating model in consultation with stakeholders and aligned with the risk management approach and compliance monitoring of non-digital risk areas
- Manages the budget for the information security function within Country/Region, monitoring and reporting discrepancies
- Manages the cost-efficient information security organization within Country/Region, consisting of direct reports and dotted line reports (such as individuals in business continuity and IT operations). This includes hiring (and conducting background checks), training, staff development, performance management and annual performance reviews

3. Strategy

- Develops an information security vision and strategy that is aligned to the country/regions' priorities and enables and facilitates the business objectives, and ensures senior stakeholder buy-in and mandate
- Develops, implements and monitors a strategic, comprehensive information security program to ensure appropriate levels of confidentiality, integrity, availability, safety, privacy and recovery of information assets owned, controlled or/and processed by the organization
- Assists with the identification of non-IT managed IT services in use ("citizen IT") and facilitates a corporate IT onboarding program to bring these services into the scope of the IT function, and apply standard controls and rigor to these services; where this is not possible, ensures that risk is reduced to the appropriate levels and ownership of this information security risk is clear
- Works effectively with business units within country/region to facilitate information security risk assessment and risk management processes, and empowers them to own and accept the level of risk they deem appropriate for their specific risk appetite

4. Framework Development

- Develops and enhances an up-to-date information security management framework based on the following: International Organization for Standardization (ISO) 2700X, ITIL, COBIT/Risk IT and National Institute of Standards and Technology (NIST) Cybersecurity Framework, PCI-DSS
- Creates and manages a unified and flexible, risk-based control framework to integrate and normalize the wide variety and ever-changing requirements resulting from global laws, standards and regulations
- Develops and maintains a document framework of continuously up-to-date information security policies, standards and guidelines. Oversees the approval and publication of these information security policies and practices
- Creates a framework for roles and responsibilities with regard to information ownership, classification, accountability and protection of information assets
- Facilitates a metrics and reporting framework to measure the efficiency and effectiveness of the program, facilitates appropriate resource allocation, and increases the maturity of the information security, and reviews it with stakeholders at the executive and board levels

5. Collaborative Functions

- Provides input for the IT section of the company's code of conduct
- Creates the necessary internal networks among the information security team and line-of-business executives, corporate compliance, audit, physical security, legal and HR management teams to ensure alignment as required
- Builds and nurtures external networks consisting of industry peers, ecosystem partners, vendors and other relevant parties to address common trends, findings, incidents and cybersecurity risks
- Liaises with external agencies, such as law enforcement and other advisory bodies, as necessary, to ensure that the organization maintains a strong security posture and is kept well-abreast of the relevant threats identified by these agencies
- Liaises with the enterprise architecture team to build alignment between the security and enterprise (reference) architectures, thus ensuring that information security requirements are implicit in these architectures and security is built in by design

6. Operational Functions

- Creates a risk-based process for the assessment and mitigation of any information security risk in the ecosystem consisting of supply chain partners, vendors, consumers and any other third parties
- Works with the compliance staff to ensure that all information owned, collected or controlled by or on behalf of the company is processed and stored in accordance with applicable laws and other global regulatory requirements, such as data privacy
- Collaborates and liaises with the data privacy officer to ensure that data privacy requirements are included where applicable
- Defines and facilitates the processes for information security risk and for legal and regulatory assessments, including the reporting and oversight of treatment efforts to address negative findings
- Ensures that security is embedded in the project delivery process by providing the appropriate information security policies, practices and guidelines
- Oversees technology dependencies outside of direct organizational control. This includes reviewing contracts and the creation of alternatives for managing risk
- Manages and contains information security incidents and events to protect corporate IT assets, intellectual property, regulated data and the company's reputation
- Monitors the external threat environment for emerging threats, and advises relevant stakeholders on the appropriate courses of action
- Develops and oversees effective disaster recovery policies and standards to align with the enterprise business continuity management (BCM) program goals, with the realization that components supporting primary business processes may be outside the corporate perimeter
- Coordinates the development of implementation of incident response plans and procedures to ensure that business-critical services are recovered in the event of a security event; provides direction, support and in-house consulting in these areas
- Facilitates and supports the development of asset inventories, including information assets in cloud services and in other parties in the organization's ecosystem

KNOWLEDGE & SKILLS

- Knowledge and understanding of relevant legal and regulatory requirements, such as:

  International Organization for Standardization (ISO) 2700X, ITIL, COBIT/Risk IT and National Institute of Standards and Technology (NIST) Cybersecurity Framework, PCI-DSS.
- Knowledge of common information security management frameworks, such as ISO/IEC 27001, ITIL, COBIT as well as those from NIST, including 800-53 and Cybersecurity Framework Sound knowledge of business management and a working knowledge of information security risk management and cybersecurity technologies.
- Up-to-date knowledge of methodologies and trends in both business and IT.
- Demonstrated experience and success in senior leadership roles in risk management, information security, and IT or OT security.
- Degree in business administration or a technology-related field, or equivalent work- or education-related experience.
- Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Control (CRISC), ISO 27001 Lead Auditor/Lead Implementer or other similar credentials.

HOW TO APPLY

All interested staff should send their CV, application letter and copies of academic certificates to **ubaugandahr@ubagroup.com** addressed to;

Head of Human Capital

United Bank for Africa

Plot 2, Jinja Road

Kampala, Uganda.

Deadline for applications is 04th March 2025.