Job Description

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

Job Title
Chief Information Security Officer

Job Location
Dar es Salaam

Category
-

Job Type
Full Time

Job level
Senior Manager

Industry
Banking

Open to Expatriates
Only Open to Tanzanian Nationals

Minimum Requirements

Min Budget
-

Max Budget
-

Primary Industry
Banking: 10 Years

Secondary Industry
-

Primary Category
-

Secondary Category
-

Certificate
-

Qualification
-

Summary

The Chief Information Security Officer (CISO) is responsible for identifying, evaluating, and reporting on legal, regulatory, IT, and cybersecurity risks affecting information assets while supporting and advancing business objectives. The role requires a visionary leader with strong business management knowledge and extensive understanding of cybersecurity technologies covering the corporate network and wider digital ecosystem.

The CISO works closely with executive management to determine acceptable levels of organizational risk and proactively collaborates with business units and ecosystem partners to implement practices aligned with approved information security policies and standards. The role requires the ability to understand and communicate the impact of cybersecurity on digital business operations to the board of directors and senior stakeholders.

Responsibilities

Establish Governance and Build Knowledge

- Facilitate an information security governance structure through the implementation of a hierarchical governance program, including the formation of an information security steering committee or advisory board.
- Provide regular reporting on the current status of the information security program to enterprise risk teams, senior business leaders and the board of directors as part of a strategic enterprise risk management program, thus supporting business outcomes.
- Develop, socialize and coordinate approval and implementation of security policies.
- Work with the vendor management office to ensure that information security requirements are included in contracts by liaising with vendor management and procurement organizations.
- Direct 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.
- Understand and interact 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.
- Provide clear risk mitigating directives for projects with components in IT, including the mandatory application of controls.
- Embed Cyber Judgement across a decentralized or distributed decision-making model.

- Lead the security champion program to mobilize employees in all locations.

Lead the Organization

- Lead the information security function across the business and the Group to ensure consistent and high-quality information security management in support of the business goals.
- Determine 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.
- Manage the budget for the information security function, monitoring and reporting discrepancies.
- Manage the cost-efficient information security organization, consisting of direct reports and dotted line reports (such as individuals in business continuity and IT operations).
- Manage hiring, background checks, training, staff development, performance management and annual performance reviews.

Set the Strategy

- Develop an information security vision and strategy aligned to business priorities and objectives while ensuring senior stakeholder buy-in and mandate.
- Develop, implement and monitor a strategic, comprehensive information security program to ensure appropriate levels of confidentiality, integrity, availability, safety, privacy and recovery of information assets.
- Identify non-IT managed IT services in use and facilitate corporate IT onboarding programs to bring services into the scope of IT governance and apply standard controls.
- Ensure information security risks are reduced to appropriate levels and ownership of risks is clearly established.
- Work effectively with business units to facilitate information security risk assessment and risk management processes.
- Empower business units to own and accept the level of risk appropriate to their risk appetite.

Develop the Frameworks

- Develop and enhance an up-to-date information security management framework.
- Create and manage a unified, flexible and risk-based control framework to integrate and normalize requirements resulting from global laws, standards and regulations.
- Develop and maintain information security policies, standards and guidelines.
- Oversee approval and publication of information security policies and practices.
- Create a framework for information ownership, classification, accountability and protection of information assets.
- Establish metrics and reporting frameworks to measure the efficiency and effectiveness of the program.
- Facilitate appropriate resource allocation and increase the maturity of information security.
- Review information security maturity with executive stakeholders and the board.

Operate the Function

- Create risk-based processes for assessment and mitigation of information security risks involving supply chain partners, vendors, consumers and third parties.
- Work with compliance teams to ensure information is processed and stored according to applicable laws and regulatory requirements.
- Collaborate with the data privacy officer to ensure data privacy requirements are included where applicable.
- Define and facilitate information security risk and regulatory assessment processes.
- Monitor and oversee treatment plans addressing security findings and risks.
- Ensure security is embedded into project delivery processes through appropriate policies, practices and guidelines.
- Oversee technology dependencies outside direct organizational control and manage associated risks.
- Review contracts and develop alternatives for managing technology-related risks.
- Manage and contain information security incidents and events to protect IT assets, intellectual property, regulated data and company reputation.
- Monitor the external threat environment and advise stakeholders on appropriate actions.
- Coordinate development and implementation of incident response plans and procedures.
- Provide direction, support and consulting to ensure recovery of business-critical services during security events.

Education & Qualifications

- Master’s or bachelor’s degree in business, computer science, computer engineering, electrical engineering, system analysis or a related field of study, or equivalent experience.

Requirements

- Ten or more years of experience in a similar position.
- Ten or more years of experience in at least three disciplines, such as business, information, solution or technical architecture, application development, middleware, information analysis, database management or operations in a multitier environment

Characteristics

- Organizational savvy, with situational and contextual intelligence of the political climate of the enterprise and ability to navigate obstacles and politics.
- Balances the long-term (“big picture”) and short-term implications of individual decisions and business goals.
- Rapidly comprehends the functions and capabilities of new technologies.
- Ready to think, behave and act in an innovative consulting manner to drive digital business strategies.
- Understands and speaks the language of the business.
- Trusted and respected as a thought leader who can influence and persuade business and IT leaders.
- Comfortable, experienced and accomplished at working with business executives and able to push back in a professional and diplomatic way.
- Highly collaborative and supportive of business and its ideals and strategies.
- Highly innovative with aptitude for foresight, systems thinking and design thinking.
- Composed in the face of opposition to architectural principles, governance and standards.
- Practical in approach to problem solving and decision making.

Reporting To

Chief Operating Officer

Driving Licence

Not Required

To Apply for This Job Click Here