CRDB BANK
Tunakusikiliza

Job Title: Manager; Cybersecurity

Reporting Line- Head; Cybersecurity

Unit- Cybersecurity

Location- Head Office

Job Summary.

To be the prime contact for technical Security solution related issues, focal point for the provision of information security solutions, ensuring all aspects of Cybersecurity security controls policies and procedures are implemented and audited. Accountable for IT Infrastructure security by using technical expertise and looking for patterns and potential issues, this includes working in close connection with ICT and Bank's other departments' management.

Key responsibilities:

- Design, implement, enforce, and monitor Cyber security strategy, Cyber Security Policies, cybersecurity framework to ensure alignment with related corporate policies, and compliance by both internal (employees) and external (vendors, third parties).
- Accountable for forensic investigation of Cyber security incidents/breaches, providing regular reporting using the appropriate assurance framework.
- Champion of cyber security incident response program, ensuring that the program is tested throughout the organization.
- Accountable for the information security awareness and training program that informs and motivates workers on cyber-security matters, this includes goals/targets audiences.
- Prepare and implement cyber security budget for the bank.

- Ensure cyber resilience on the bank by having robust Disaster recovery site on the cyber security controls on all layers of security.
- Provide technical advice, proposing and implementing solutions and processes to continuously reduce the Cyber security risks. This involves working with different units in the department to reduce cyber security risk. From technical controls to policies (and everything in between).
- Accountable for hardening (this includes patching) of organization’s IT assets before promoted to production environment. Formal checklist will be used for installation/changes of any configuration in the banks environment this is for a new/existing setup, this includes but not limited to servers, workstations, databases, audio visuals and network devices, as per current hardening standards of the bank.
- Accountable for effective security controls implementation to all ICT systems environment, this includes vulnerability assessment and penetration tests (VAPT).
- Responsible for overall in charge of all cyber security systems, tools, processes and people, ensuring their design and operational effectiveness.

Experience, Knowledge, and Skills Requirements

- Bachelor’s Degree in Computer Systems, Technology or any other equivalent and relevant qualification from an accredited institution.
- Minimum of 5 years of experience in Cybersecurity.
- At least 1 ICT Security professional certifications, CISM, CISA, CISSP, CEH etc.
- Expert knowledge of current and emerging cyber security issues.
- Management of a complex IT Infrastructure within large enterprise level financial organization.
- Contingency and Disaster Recovery Planning.
- Up-to-date knowledge of different systems used in the Banking environment.
- Ability to think ahead and anticipate problems, issues, and solutions.
- Experience providing Cybersecurity focused Enterprise Architecture and strategy.
- Windows Operating systems and Active Directory Management.
- Extensive Cyber knowledge across areas such as; IT desktop applications, Computer technology, Operating systems (Windows, LINUX, Red hat, AIX ...), Networking & Database technology, IT Security & Virtualization, Microsoft Server and Supporting Services, Cybersecurity tools, processes, and systems.

Deadline 25th August 2023

Apply Here