Designation	: **Security Analyst**
Reporting Line	: **Manager Policy and Compliance**
Business Unit	: Risk
Location	: Lusaka

Job Purpose : To operationalize the Cyber Security Strategy by assessing potential threats, monitor network and system activity, coordinate the implementation and management of safety protocols, and research emerging threats to determine the best response to them.

KEY OUTPUT & RESPONSIBILITIES

❖ IS strategy implementation and alignment
- Develop implementation plan and methodology for the IT Security Assessment to ensure that the assessments are based on acceptable standards and frameworks.
- Collaborate with IT Department in the development of the IT Security Maturity Roadmap to ensure that the Cyber Security Strategy is operationalized and monitored.

❖ Updated Information Security Policies and Frameworks
- Participate in the development of IS Policies and Security Framework based on Information Security Standards and Best Practices to ensure that they remain relevant
- Participate in the Identification and development of assessment metrics based on Regulatory and Legal Frameworks to ensure alignment with regulatory bodies

❖ Operationalization of Policies, Regulatory Frameworks and Acts
- Perform Periodic Reviews of operations as guided by the Information Security Policy and security standards and frameworks to ensure that the processes and systems are secure
- Develop and publish the Compliance Assessment Metrics to ensure that the baselines are based on approved standards and policies
- Develop and Deliver the Information Security Awareness / Training to ensure that the users in the Bank are made aware of their roles and responsibilities in the Information Security Management System of the Bank.

❖ Up-to-date IT Risk Register
- Communicate risks and provide recommendations to mitigate risks to management so that decisions can be made to ensure the security of information systems.

❖ Coordinate Timely Closure of Audit Findings
- Review and coordinate closure of the Vulnerability Assessment findings, IS Incidents, Audit Findings & Penetration Tests Findings to ensure that all threats are mitigated timely.
- Tracking of all findings and issues from internal and external audits to ensure quality closure and minimise repeat findings.

❖ Accurate, timely reporting
- Identify trends and make recommendations on improvements and where possible breaches could occur in the future to avoid materialisation of the threats which may cause financial losses.
- Participation in business and IT projects to provide input into the IT projects and assure security.

❖ Stakeholder Relationship Management
- Meet regularly with business stakeholders to operationalize the IS Policy
- Build and maintain good relationships with vendors / outsourced third parties to resolve specific issues and manage them in line with information security requirement
- Effective teamwork, self-management and alignment with bank values

Qualifications & Experience
- Grade 12 School Certificate with 5 credits, English and Mathematics inclusive
- Degree in I.T or in a related field
- 2 – 3 years' IT experience with exposure to security frameworks implementations and monitoring
- Security Certifications also preferred: CISSP/CCSA/CEH/ISO27001 Lead Audit
- Understanding of the Banks IT infrastructure, Applications, incident management and troubleshooting

Interested Applicants who meet the job requirements should email their CV's to e-mail address jobs-zm@bancabc.co.zm Please note that only shortlisted candidates will be contacted. **Clearly state the position you are applying for in the subject field**.
Closing date:
Tuesday, 21st March, 2023