Designation : **Manager : Risk & Resilience**	Designation : **Manager : Policy & Compliance**
Reporting Line : Head : Information Security	Reporting Line : Head : Information Security
Business Unit : Risk	Business Unit : Risk
Location : Lusaka	Location : Lusaka
Job Purpose : In collaboration with stakeholders, support the drive of continuous assessment of Information Security and Information Technology risks across Atlas Mara Asset portfolio. Identifying, assessing, and prioritizing risks and mitigations to continuously improve the resilience of Bank's Assets.	Job Purpose : In collaboration with stakeholders, support the development and oversee the implementation of Information Security and Information Technology control systems to prevent or deal with violations of policies, standards and procedures. Evaluating the efficiency of these controls and improve them continuously.
KEY OUTPUT & RESPONSIBILITIES ❖ IS strategy implementation and alignment • Participate in the development of the Information Risk strategy to ensure that it is aligned with the business objective and that there is alignment between Risk and IT Departments. • Review, align and communicate compliance performance for satisfactory audits and ensuring that repeat findings are minimized. • Plan and implement methodology for the IT Security Assessment to ensure that assessment is based on current security frameworks. • Collaborate with IT Department in the development of the IT Security Maturity Roadmap to ensure that Cyber Security posture is continuously improved and is part of the strategy. ❖ Updated IT Business Continuity and Security Risk Assessment Framework • Review of Information Security Policies against standards ensuring they remain relevant. • Identify and develop Business Continuity and Resilience assessment metrics based on Regulatory and Legal Frameworks the organization is compliant with frameworks. • Ensure that the Business Continuity Plans are in place and monitored to provide assurance that the organization can recover in case of a disaster. ❖ Operationalization of Policies, Regulatory Frameworks and Acts • Perform Periodic Reviews of operations as guided by the Information Security Policy so that IT implementations are secure and based on approved Policies. • Develop and publish the Risk and Resilience Assessment Metrics to manage stakeholders and provide for continuous improvement. ❖ 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. • Perform Quarterly Compliance Assessments and report status on Monthly Basis as part of the decision-making cycle for secure and compliant system implementations. ❖ 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 the threats are managed and mitigated. • Tracking of all findings and issues from internal and external audits to ensure quality closure of issues. ❖ Accurate, timely reporting	**KEY OUTPUT & RESPONSIBILITIES** ❖ IS strategy implementation and alignment • Participate in the development of the Information Risk strategy to ensure that it is aligned with the business objective and that there is alignment between Risk and IT Departments. • Develop strategy and implementation plan for the IT Risk Compliance unit to ensure alignment between Risk and IT Departments ❖ Updated Information Security Policies and Frameworks • Develop IS Policies and Security Framework based on international Information Security Standards to ensure that they are based on best practice • Review of Information Security Policies against standards ensuring they remain relevant ❖ Operationalization of Policies, Regulatory Frameworks and Acts • Perform Periodic Reviews of operations as guided by the Information Security Policy so that the processes and systems are secure and compliant • Develop and publish the Compliance Assessment Metrics in order to guide the assessment requirements and implementation expectations as per Policy and Standards • Monthly IT Critical Process Compliance Review: Access Management, Backup and Restoration, Project Management to ensure that the processes are based on best practice and standards. • Implement the Information Security Awareness Program ❖ 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. • Perform Quarterly Compliance Assessments and report status on Monthly Basis to ensure that processes are compliant to approved policies and standards and minimise risks. ❖ 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 threats are mitigated • Tracking of all findings and issues from internal and external audits in order to ensure quality closure of issues 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 system breaches that may result in losses. • Proactive identification and resolution of flagged concerns to mitigate threats. ❖ Stakeholder Relationship Management • Provide input into the IT projects and assure security for IT implementations. • 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 group values **Qualifications & Experience** • Grade 12 School Certificate with 5 credits, English and Mathematics inclusive • Degree in I.T or in a related field • 4 – 5 years' IT experience with exposure to having led a team and working in a banking environment. • Security Certifications also preferred: IT Risk Fundamentals, CISM and CRISC • Basic understanding of the Banks IT infrastructure, Applications, incident management and troubleshooting	• Identify trends and make recommendations on improvements and where possible breaches could occur in the future to avoid system breaches that could result in losses. ❖ 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 requirements • Effective teamwork, self-management and alignment with group values **Qualifications & Experience** • Grade 12 School Certificate with 5 credits, English and Mathematics inclusive • Degree in I.T or in a related field • 4 – 5 years' IT experience with exposure to having led a team and working in a banking environment. • Security Certifications also preferred: CISM, IT Risk Fundamentals and CGEIT. • Basic understanding of the Banks IT infrastructure, Applications, incident management and troubleshooting • Knowledge of the PCI DSS, SWIFT and ISO27001 Standards will be an added advantage
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: Friday, 24th March, 2023	