BANK OF AFRICA
BMCE GROUP

JOB DESCRIPTION

Job details	
Job Title: **Officer – Information Systems Officer**	Department/Office: **Enterprise Risk**
Supervisor/Manager Title: **Head, Enterprise Risk**	Grade:
Positions reporting to this job: **None**	

Job Purpose

Development and management of an efficient BOA Kenya's Information Security Program that can identify, measure, monitor, and control the risks inherent in the Bank's ICT systems while ensuring compliance with Industry Standards and Regulations.

Responsibilities and Accountabilities

1) IT Security Governance through:
   a) Developing and ensuring adherence to the annual IT Security Annual Plan BOA Kenya's Cybersecurity Strategy.
   b) Formulation and review of ISMS, Cyber policies, and procedures.
   c) Attending various IT Security & Risk related committees i.e., Monthly IT Steering committee, KBA IT Systems, Risk and Security Sub-Committee Meetings.
   d) Implementation and enforcement of ISO 27001 framework in BOA Kenya's Security practices i.e., software development, change management.

2) IT Security Risk Management through:
   a) Developing and periodic review/monitoring of IT & Security Key Risk Indicators.
   b) Update of the IT Risk register guided by periodic risk assessments.
   c) Periodic Endpoint Security reviews for compliance and timely updates.
   d) Review of Third-party risks guided by criticality, policies and procedures and SLAs and presentation of recommendations to Management to reduce associated risks.
   e) Conducting periodic Vulnerability assessment for BOA Kenya Infrastructure and develop remediation plans with IT Unit for critical vulnerabilities.
   f) Conducting periodic IT Security Assessment for New Applications, Projects, and Tools before adoption at BOA Kenya and recommendations on mitigants.
   g) Review and approve change requests raised by IT or BOA Kenya stakeholders for key infrastructure.

3) Information Security Program Development and Management by:
   a) Development and adherence to BOA Kenya's Annual User Awareness Training Plan.
   b) Prepare and publish periodic IT Security awareness topics to BOA Kenya Staff.
   c) Research and review current Cybersecurity trends, threats updates, and reviews as applicable to BOA Kenya's Environment.
   d) Conduct Targeted user training for specific roles within the Bank e.g., SWIFT, IT, New staff as guided by criticality.

e) Prepare and review Customer awareness on Information Security
f) Prepare and manage periodic user awareness campaigns on the bank's awareness platform.

4) Information Security Incident Management through:
   a) Leading in Incident handling and reporting of IT Security related incidents to BOA Kenya Management, CBK and Group Security
   b) Guiding Investigations and follow-up on remediation of incidents in the bank – tracked in an Incident Register
   c) Reviewing and testing of incident response procedures through Scenario reviews & table-top exercises.
   d) Planning and co-ordination of IT DR/BCP activities i.e development of test cases, system testing, user training & reporting, implementation, and enhancements.

5) System Access Control Management by:
   a) Conducting periodic User Access and privileged accounts rights reviews on Bank systems for anomalies.
   b) Conducting periodic USB, VPN and BYOD access reviews.
   c) Reviewing Bank systems for compliance relates to password policies, session management, authentication, and authorization.

6) ICT Risk & Security Reporting:
   a) Prepare and report monthly to IT steering committee on BOA Kenya's security status and activities.
   b) Prepare Quarterly Security report to Board which is presented by the Head, Enterprise Risk.
   c) Prepare Monthly Security report for consumption by stakeholders
   d) Follow up and closure of audit findings through weekly meetings with IT and Group security.

Key Performance Indicators

- Monthly user awareness & training (1 active campaign on cyber security awareness platform, 4 email publications).
- Monthly endpoint security reviews of antivirus status for compliance
- Project risk assessments for risk identification as guided by the Bank's project plans.
- Monthly vulnerability assessments and remediation.
- Annual and quarterly IT DR exercise testing, restoration, and failovers for business continuity.
- Quarterly access management and reviews.
- Monthly incident reporting.
- Weekly audit follow-up and closure.
- Monthly & quarterly reporting to IT Steering committee, Management & Board.
- Monthly IT security report on intrusions, endpoint security compliance, security trends and unit activities.

- Quarterly regulatory reporting & returns to CBK and KEPSS.
- Annual policy & procedure development and approval.
- Annual security tools Implementation and renewals reviews.

Minimum Requirements

a) A Bachelor's degree in an ICT related field.
b) Minimum 3 years' experience in ICT/ Security related roles.
c) IT Certifications – CCNA – security.
d) Information Security certifications (requisite, the more the added advantage)
   - CISSP (Certified Information Systems Security Professional)
   - Certified Ethical Hacker (CEH).
   - CISA (Certified Information Security Auditor)
   - CCISO (Certified Chief Information Security Officer)
   - CISM (Certified Information Security Manager)
   - ISO 27001 Lead Implementer

Competencies and Attributes

- **Integrity –** Honest, Strong moral principles and able to earn other people's trust.
- **Competence and due professional care –** Ability to carry out task in accordance with the set standards.
- **Good Communication (written and verbal) -** Ability to effectively communicate to target audience.
- **Analytical** – Ability to identify and solve problems
- **Dynamic/Adaptable** - Ability to adapt quickly to new and diverse environments including working with people from diverse cultural backgrounds
- **Team Player** – Ability to work with others in the department or BOA Kenya, share duties and seek opinions of others in the day-to-day activities.
- **Initiative & Innovative** – Takes initiative and ability to think outside the box in creating new and better ways or solutions in Information Security.

Relationships and working contacts

Internal Stakeholders: Board of Directors, Management BOA Kenya staff.
External Stakeholders: Service providers, Regulators

Work Environment

Office set up

Application Criteria

Send your Current CV and brief application Letter to recruitment@boakenya.com Application deadline is Monday 24th, October 2022.