Job Title:	Manager, IT Security	Reports to:	Head of IT and Projects
Unit:	IT	Department:	IT & Projects
Grade:		Date:	
Job Holder:		Supervisor:	
Signature		Signature:	

Job Purpose Statement
Reporting to the Head of IT and Projects the Manager IT Security shall be responsible for the Bank's Information Technology security program with the main objective of protecting CIBKE's information systems, network and infrastructure from external and internal threats.
Key Responsibilities
Financial Budget Planning: collaborate with the Head of It and Projects and various stakeholders to plan the IT security budget. This involves estimating the financial resources required to address security needs for the upcoming fiscal year. Expense Monitoring: Continuously monitor and manage expenses related to security projects and initiatives to ensure they remain within budget. If there are deviations, take corrective actions as needed. Long-Term Planning: Consider long-term financial planning for security, including multi-year budgets that account for evolving threats and technology. **Customer** Policy Development**:** Develop, implement, and enforce IT security policies and procedures for internal customers to ensure compliance with security standards and best practices. Access Control**:** Manage user access to systems, applications, and data, ensuring that internal customers have the appropriate level of access based on their roles and responsibilities. Incident Response**:** Develop and implement an incident response plan and lead incident response efforts in the event of security breaches or incidents, working closely with internal stakeholders.

Internal Business Process

Data Protection: Implement measures to protect sensitive data that is part of business processes. This includes encryption, data loss prevention, and secure data handling practices.

Business Continuity and Disaster Recovery: Develop and maintain business continuity and disaster recovery plans to ensure that critical business processes can be quickly resumed in the event of a disruptive incident or disaster.

Audit: Ensure appropriate action plans and delivery dates are in place to address any open internal or external audit items and track these actions to completion (Closer).

Functional responsibilities

- Build the security infrastructure architecture to help manage, operate, maintain, and monitor adherence to IT Security architecture and system wide policies.
- Oversee the development and management of security controls, defenses and countermeasures to prevent and safeguard the security, integrity, and confidentiality of all corporate and customer data.
- Ensure annual regulatory and compliance needs are met and respond to audit requests for information related to IT security, on application, data, network, Services, endpoint, and servers, in order to ensure effective controls according to business/compliance/regulation requirements.
- Participate and recommend improvements to policies, processes and procedures and manage their implementation to ensure all relevant procedural / legislative requirements are fulfilled.
- Supervise the day-to-day operations of the IT Security team by providing guidance in the related area, encouraging teamwork, and facilitating related professional work processes in order to achieve high performance standards.

Our Values
• Innovation and Creativity • Integrity • Passion and Commitment • Customer Service Excellence • Transparency and Accountability • Teamwork

Job Specification
Academic Bachelor's degree in information technology, Computer Engineering, Computer Science or equivalent. Masters in IT related field is a plus. **Professional Qualifications & Experience** Certified Information Systems Security Professional (CISSP) Certified Information Systems Auditor (CISA) Security frameworks and best practices (e.g., PCI, ISO27K, NIST Information Technology Infrastructure Library (ITIL) **Desired Work Experience** Minimum 8 – 10 years of experience in Systems and Information Security administration with at least 3-5 years professional experience in a managerial role.

Reporting Relationships: jobs that report to this position directly and indirectly	
Functional Reports	• All IT Security Staff
Administrative Reports	• All IT Security Staff

Stakeholders: key stakeholders that the position holder will need to liaise/work with to be successful in this role.	
Internal	• All Bank Departments.
External	• IT Vendors, Service Providers and CBK.

Decision Making Authority /Mandates/Constraints: the decisions the position holder is empowered to make *(Indicate if it is Operational, Managerial or Strategic)*

Operational, Managerial and Strategic.

Ideal Job Competencies: Technical Competence	
Technical	Experience designing, implementing, and maintaining large scale security solutions
	Proven Experience in Security Solutions troubleshooting, monitoring tools, alarm conditions, and escalation processes and procedures
	Experience with enterprise security architecture and software like IPS/IDS, AV, Vulnerability scanners, DLP, web security and email security, Information Security frameworks and best practices (e.g. PCI, ISO27K, NIST)
	Strong Knowledge of Defense-in-Depth mechanism
	Outstanding performance of duties and exceeding expectations in positions that require strong analytical, problem-solving, decision-making, team building, and leadership skills.
	Knowledge and skills on encryption, VPN is essential.
	Extensive knowledge of the Financial and Banking sector
	Extensive Fraud and Operational risk knowledge

Ideal Job Competencies: Behavioral Competence	
Technical	Dynamic, analytical, and self-driven individual with the ability to work under pressure
	Strong People, Project, and Time Management Skills
	Hardworking, strategically minded individual with excellent organizational and planning skills