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

Job Purpose Statement

The role involves management and monitoring the security of the infrastructure and platforms to ensure the principles of confidentiality, integrity and availability are upheld. The responsibilities include implementing approved security measures according to CIBs' policies, standard operating procedures, and compliance requirements.

Key Responsibilities

Financial

- Ensure the availability of bank end to end IT security controls covering perimeter, Branches, DMZ, Access layer, 3rd Party, Data Centre firewalls and endpoints to make sure that a unified and complaint policy is applied across the organization.
- Ensure the availability and efficient operations of banks' end to end network security solutions such as firewalls, VPNs, Intrusion Detection Systems (IDS), to provide the required levels of assurance regarding the effectiveness of banks' security measures and approved controls.
- Assist with implementation of the Bank's strategy, roadmap, and delivery plans for IT Security in coordination with the network, applications, and information security teams.
- Monitor, report and provide the network officer with network security trends and advice to changes in policy, procedures, and tools to enhance the network security posture.
- Provide technical IT security expertise to the Bank' projects and to provide the required levels of assurance regarding the readiness of the banks' security controls.
- Review and critique network security solutions, in full alignment with the network officer, in order to be able to evaluate the alignment to operational and mission requirements over a range of metrics including scalability, maintainability, security, reliability, flexibility, availability, and manageability.
- Monitor the performance of security applications in scope and to ensure a healthy and risk-free secure network connectivity through the entire organization.

Customer

- Build the IT security infrastructure architecture in order to help manage, operate, maintain, and monitor adherence to the 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.
- Contribute to and at times lead training sessions on technology and especially IT security related topics, in order to enhance the overall organization learning and security awareness curve.
- Provide security technical expertise for Project Management to support the bank's Business Strategic Projects and, in order to create and maintain a secure Software Development Life

Cycle (SDLC) in the organization that complies with Business Strategic objectives, policies, procedures, rules and regulations.

Internal Business Process.

- Ensure that custom Applications and IT Operations management tools, such as network management and log management have the appropriate security measures built into them at deployment, in order to maintain unified security measures and business reporting mechanisms are in place.
- Ensure the requirements for new tools are integrated efficiently and effectively with the existing tools and technologies, gathering all related requirements and guide/recommend the right integration pattern, taking into consideration the impact to the environment and standards to ensure effective security architecture and controls over enterprise applications.
- Oversee and provide direction for risk assessment, testing and deployment of security controls and standards, root cause analysis, security scans, incident handling, vulnerability assessments, and documentation.
- Provide technical expertise and guide the administration of security tools that control and monitor information security, in order to keep business up and running seamlessly.
- Create and maintain monthly security reports and dashboards across various IT Security solutions, documentation for security related activities and metrics/KPIs reporting, in order to be presented to the respective stakeholders/committees as needed.
- Advocate secure computing practices and procedures, and communicate IT Security best practices, in order to keep the business secured proactively against threats.

Functional responsibilities

- Provide the required level of support to all managed systems and platforms including: Endpoint protection, Enterprise Mobility solutions, Encryption, Endpoint Sandboxing solutions, Endpoint Detection and Response, Endpoint Data Classification and others, in order to maintain business operations according to the approved service level agreement.
- Ensure the availability of Secure Remote access and Work from Home Arrangement technologies, and Endpoint Detection/Response, to provide the required levels of assurance that Bank Work from Home Arrangements are being handled and operational in a secure way according to industry best practice and information security policies.
- Ensure proper functionality of managed endpoint and mobile solutions through marinating effective coordination with support vendors for resolve issues impacting availability, in order to keep the solutions fully compliant with the current architecture and incident response requirements.
- Manage the reporting and tracking of issues related to endpoint and mobile security gaps, data leakage incidents, mobile devices security effectively and efficiently, in order to ensure proper implementation and operations according to organization objectives, solution best practice and compliance/regulation requirements.
- Ensure compliance with all relevant CBK regulations, banking laws, AML regulations and internal CIB policies and code of conduct in order to maintain CIB's sound legal position and mitigate any potential risks.

Our Values

Customers First

- We listen proactively to our customers to understand their needs and expectations.
- We integrate the voice of the customers in new product and service developments.

- We go the extra mile when serving our customers.
- We optimize our processes to deliver the highest value and a seamless experience to our customers.
- We measure and benchmark customer engagement KPIs and integrate them into our leadership evaluation.

Lead The Market

- We strive to offer the best products and the highest quality service.
- We aim to invest further to strengthen and enhance our market position.
- We provide an environment to our employees where everyone can give their absolute best.
- We train and equip our employees to be best prepared for a constantly evolving financial service market.
- We are a role model in implementing national initiatives and regulatory guidelines.

Agility

- We embrace a changing market environment and respond decisively and swiftly.
- We release new products and pilots quickly to test and optimize them in a real environment.
- We are open to trying new things, but rigorous in evaluating our success and happy to accept mistakes.
- We collaborate proactively within cross-functional teams and limit vertical hierarchies to a minimum.
- We leverage technology to support, facilitate, and automate our processes and time to market.

Integrity

- We hold ourselves accountable to a higher standard of responsibility.
- We are doing the right things, even if it is commercially less attractive.
- We communicate clearly what we can deliver and keep our word.
- We do things right and create solutions that work.
- We fully comply with all regulatory and compliance standards and apply zero tolerance to misconduct.

Job Specification

Academic

- Bachelor's degree in engineering, Information Technology, Computer Science or equivalent.

Professional Qualifications & Experience

- At least one Security certification from the list: CEH (Certified Ethical Hacker), CompTIA Security+, OSCP (Offensive Security Certified Professional), SSCP (Systems Security Certified Practitioner).
- At least one Networking Certification; CCNA: Cisco Certified Network Associate; CCNP: Cisco Certified Network Professional.
- .
- Proven Experience in IT Security Solutions deployment, troubleshooting, 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)
- Good Knowledge of Networking, preferably CISCO products and technologies.
    - Routing & Switching (Routing protocols such as EIGRP, OSPF, BGP, and Instant Switches).
    - Data Center Security Products (Next Generation Firewalls, IPS).
    - Network Security techniques (Encryption, ISE, NAC, dot1x, device hardening).

- Strong Knowledge in Defense-in-Depth mechanism.

Desired Work Experience

Minimum 2-4 years of experience in IT Security

Reporting Relationships: jobs that report to this position directly and indirectly	
Functional Reports	none

Stakeholders: key stakeholders that the position holder will need to liaise/work with to be successful in this role.	
Internal	All Departments in the Bank
External	Third Party vendors/Technical support vendors

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

Managerial

Ideal Job Competencies: Technical Competence

- Excellent written and verbal communication skills.
- Good understanding of authentication mechanisms.
- Strong Time Management Skills.
- Strong Problem-Solving Skills.
- Demonstrated ability to implement process, create SOPs, and write effective documentation

Ideal Job Competencies: Behavioral Competence

Problem-Solving and Analytical Skills:

- Analytical Thinking Level 3.

Communication Skills:

- Customer Service Orientation Level 4.

Team Collaboration:

- Impact & Influence Level 3.
- Management of Performance Level 2
- Organizational Commitment Level 3.

Attention to Detail:

- Meticulous in documenting network configurations, procedures, and policies.
- Ensures accuracy and compliance in network audits and assessments.

Adaptability and Flexibility:

- Ability to adapt to changing technology and business environments.
- Willingness to work outside regular hours for network maintenance and emergencies.