

Job Title:	Security Engineer	Reports to:	Senior Manager, Security Engineering and Operations
Unit:	Information Security	Department :	Information Technology
Grade:	Band 5	Date:	August 2023
Job holder:		Supervisor:	
Signature:		Signature:	

Job Purpose Statement

This role will provide technology security assurance, to ensure that existing and new systems, services and products meet the security compliance threshold. The jobholder will work closely with IT teams to ensure that existing systems meet Bank's security requirements as well as best practices.

Key Accountabilities (Duties and Responsibilities)

Perspective	% Weighting (to add up to 100%)	Output
Security assessments	70%	<ul style="list-style-type: none"> Review and recommend secure system configuration for servers, workstations and network devices and provided security recommendations to mitigate loss of confidentiality, integrity and availability of data Conduct security assessments and reviews on existing systems (IT &OT) and products, ensuring that they comply with the Bank's security standards and policies. Interpret and communicate security controls accurately to IT teams with regard to system security posture, policy updates and configuration for information systems. Liaise with IT teams to validate closure of remediation actions done on identified gaps. Participate in planning, design and execution of cyber security assurance Plan.

Development	20%	<ul style="list-style-type: none"> • Support the establishment of program control processes to ensure cyber risk mitigations are put in place. • Proactively participate in technical solution design for new systems, ensuring that security requirements are well defined. • Participate in the creation of new and improvement of existing enterprise security policies, standards, baselines, guidelines and procedures.
Change Management	10%	<ul style="list-style-type: none"> • Participate in security assessments and testing reports as inputs in the Change Management approval process.

Job Dimensions

Reporting Relationships: jobs that report to this position directly and indirectly	
Direct Reports	None
Indirect Reports	None

Stakeholder Management: key stakeholders that the position holder will need to liaise/work with to be successful in this role.	
Internal IT Department Enterprise Project Management Department Enterprise Risk & Compliance Department	External Information Security Consultants

Decision Making Authority /Mandates/Constraints: the decisions the position holder is empowered to make <i>(Indicate if it is Operational, Managerial or Strategic). Please also highlight any budgetary control responsibility if applicable for the role.</i>
Operational – security compliance assessments, testing practices Management- Vendor management

Work cycle and impact: time horizon and nature of impact (Planning) <i>(e.g. Less than 1 week, 2 weeks, 2 weeks – 1 month, 1month – 3 months, 3-6 months, 6-12 months, above 1 year)</i>
3-6 months

Ideal Job Specifications

- Bachelor's Degree in, Information Systems, Computer Science, Information Security or related field required
- Minimum 2-5 years working experience, with at least 2 years' experience in a busy IT security environment.
- Knowledge of secure configuration and change management practices.
- Working knowledge of databases, operating systems and web applications technologies.
- Certification in systems audit or security related area, such as CEH, CISA, CISM or CISSP
- Experience in working with various vulnerability assessment & penetration testing tools.
- Working knowledge of IT systems security hardening practices
- Prior experience working within a financial service organization will be an added advantage
- Knowledge in DevOps technologies and practices will be an added advantage

Ideal Job competencies

Technical Competencies	
	<ul style="list-style-type: none">• Technical skills to effectively perform IT security management activities/tasks in a manner that consistently achieves established quality standards or benchmarks.• Knowledge of information security domains• Conceptual understanding of Vulnerability and Risk Assessments.• Working knowledge of system security controls on multiple operating systems (Windows, Linux)• Practical understanding of common TCP/IP-based services, including DNS, DHCP, HTTP, FTP, SSH, SMTP• Knowledge and application of modern IT security management practices in financial services industry to proactively define and implement security quality improvements in line with technological and product changes.• Performance management to optimize personal productivity.• Knowledge and effective application of all relevant banking policies, processes, procedures and guidelines to consistently achieve required compliance standards or benchmarks.
Behavioural Competencies	
	<ul style="list-style-type: none">• Interpersonal skills to effectively communicate with and manage expectations of all team members and other stakeholders who impact performance.• Self-empowerment to enable development of open communication, teamwork and trust that are needed to support true performance and customer-service oriented culture.• Demonstrable integrity and ethical practices