Job Title:	Infrastructure Security Engineer	**Reports to:**	Senior Manager, Security Engineering
Department/ Sub-department:	Information Security, Information Technology	**Division:**	Technology & Operations
Grade:	Band 5	**Date:**	
Job holder:		**Supervisor:**	
Signature:		**Signature:**	

Job Purpose Statement
The Infrastructure Security Architect & Engineer role focuses on designing, implementing, and maintaining secure infrastructure solutions to safeguard the Bank's IT environment. This role involves developing robust security architectures, integrating security into infrastructure projects, and supporting compliance efforts. The position requires hands-on experience in securing hybrid environments, including on-premise, cloud, and virtualized systems, while collaborating with various teams and vendors to enhance the organization's security posture.

Key Results Areas		
Perspective	**% Weighting** *(to add up to 100%)*	**Output**
Security Architecture Design and Implementation	30%	• Design and implement secure infrastructure solutions, including cloud, on-premises, and hybrid environments. • Integrate security requirements into infrastructure and application development processes. • Collaborate with project teams to ensure secure design and deployment of IT systems. • Assess emerging technologies and provide recommendations to improve security and efficiency.
Infrastructure Hardening and Optimization	30%	• Develop and enforce security baselines for servers, networks, storage, and virtualization platforms.

		• Optimize existing infrastructure for enhanced security, scalability, and performance. • Continuously refine policies and configurations to adapt to evolving threats. • Support vulnerability management by identifying and addressing infrastructure-level risks.
Operational Management and Incident Support	20%	• Administer and manage infrastructure security tools, such as firewalls, IDS/IPS, endpoint protection, and identity management platforms. • Collaborate with the SOC and IT operations teams to investigate and resolve security incidents. • Maintain comprehensive documentation for configurations, procedures, and incident responses. • Periodic Infrastructure security assessments/Reviews
Compliance Support and Reporting	20%	• Ensure infrastructure aligns with regulatory requirements and industry standards (e.g., ISO 27001, NIST etc...). • Generate periodic security coverage reports and metrics for stakeholders. • Support audits and compliance reviews by providing detailed evidence and insights. • Work closely with third-party solution providers to implement and validate secure infrastructure solutions.

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 & Compliance Risk Department Internal Audit	**External** External Auditors Regulators

Stakeholder Management: key stakeholders that the position holder will need to liaise/work with to be successful in this role.	

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

Operational , Technical

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

6-12 months

Ideal Person Specifications

- Bachelor's degree in Computer Science, Information Technology, Cybersecurity, or a related field.
- 2-5 years of experience in infrastructure security, Cybersecurity architecture, and cybersecurity engineering.
- Hands-on expertise with security tools and platforms such as IDS/IPS, firewalls, VPNs, SIEM, and cloud security solutions.
- Proficiency in scripting or automation (e.g., Python, PowerShell, Ansible) is a plus.
- Relevant certifications such as CISSP, CISM, CCSP, AWS Certified Security Specialist, or Azure Security Engineer Associate are preferred.

Behavioural Competencies

- Strong technical acumen and problem-solving abilities to design and implement secure systems.
- Effective collaboration skills for working with cross-functional teams and third-party vendors.
- Proactive approach to identifying and mitigating risks in complex IT environments.
- Excellent communication skills for conveying security concepts to technical and non-technical stakeholders.
- Adaptability to keep pace with rapidly evolving technologies and security threats.