Job Title:	Cybersecurity Engineer	**Reports to:**	Senior Manager, Cybersecurity Engineering
Department/ Sub-department:	Information Security, Information Technology	**Division:**	Technology & Operations
Grade:	Band 4	**Date:**	
Job holder:		**Supervisor:**	
Signature:		**Signature:**	

Job Purpose Statement
This role safeguards the bank's digital assets by implementing, managing, and optimizing advanced security tools and platforms. Responsibilities include deploying and optimizing security solutions, administering tools, supporting compliance processes, addressing vulnerabilities, and collaborating extensively with third-party solution providers and vendors to defend the bank. The role ensures robust protection against evolving threats through cross-team collaboration while maintaining seamless operations.

Key Results Areas		
Perspective	**% Weighting** *(to add up to 100%)*	**Output**
Implementation of Security Solutions	30%	• Deploy and configure advanced security tools and platforms to enhance the bank's defenses. • Integrate security solutions with existing infrastructure, minimizing operational disruptions. • Collaborate with third-party vendors to ensure successful deployments of security solutions and alignment with business objectives.
Optimization, Vulnerability Management, and Reporting	30%	• Continuously refine and optimize security tools and policies to stay ahead of emerging threats. • Perform vulnerability assessments and implement effective remediation strategies. • Prepare and share periodic coverage and performance reports to enhance security posture.

		• Work closely with vendors to ensure timely updates, patches, and resolution of technical issues.
Compliance Support and Collaboration	20%	• Support compliance initiatives by delivering actionable insights and reports aligned with regulatory requirements. • Collaborate with IT, DevOps, SOC teams, and external partners to strengthen security measures and meet compliance standards.
Threat Response and Documentation	20%	• Detect and respond to potential security incidents using established protocols and tools. • Maintain detailed, up-to-date documentation for security configurations and operational procedures. • Present performance metrics and security insights to stakeholders, facilitating informed decision-making.

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

Decision Making Authority /Mandates/Constraints: the decisions the position holder is empowered to make *(Indicate if it is Operational, Managerial or Strategic)*.
Operational –procedures and policy maintenance and implementation, audit management and planning

Work cycle and impact: time horizon and nature of impact (Planning) *(e.g. Less than 1 week, 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. • 2-4 years of experience in implementing and managing advanced security solutions. • Proven expertise in tools such as XDR, DAM, SIEM, PAM, PIM, WAF, IDS, IPS, and FIM. • In-depth understanding of network protocols, security frameworks, and IT infrastructure. • Proficiency in scripting and automation (e.g., Python, PowerShell) is a plus. • Relevant certifications (e.g., CISSP, CISM, CEH, CompTIA Security+, or vendor-specific credentials) are preferred.

Behavioural Competencies
• Strategic thinking and problem-solving skills to address complex cybersecurity challenges. • Strong communication and teamwork capabilities to foster cross-functional collaboration. • Meticulous attention to detail and a proactive approach to risk identification and mitigation. • Adaptability to rapidly learn and implement emerging tools and technologies.

This JD is signed-off with reference having been made to the organisation's core values and aligned competencies against these values.