Job Title:	Security Operations Centre (SOC) Specialist	**Reports to:**	Senior Manager, Cybersecurity Operations Center
Department/ Sub-department:	Information Security, Information Technology	**Division:**	Technology & Operations
Grade:	Band 5	**Date:**	
Job holder:		**Supervisor:**	
Signature:		**Signature:**	

Job Purpose Statement
The SOC Specialist plays a crucial role in monitoring, detecting, and responding to cybersecurity threats and incidents. This role requires technical expertise in cybersecurity tools and processes, strong analytical skills, and the ability to operate effectively in a dynamic, high-pressure environment. This Role will be a specialised Role for **Incident response** and will act as an escalation point for SOC Analysts.

Key Results Areas		
Perspective	**% Weighting** *(to add up to 100%)*	**Output**
Security Monitoring, Reporting and Incident management	60%	• Monitor and analyse network traffic, system logs, and alerts to identify potential security incidents. • Respond to cybersecurity incidents, including analysis, containment, eradication, and recovery. • Conduct root cause analysis of security incidents to prevent future occurrences. • Collaborate with other teams to enhance threat detection capabilities and improve overall security posture. • Perform threat hunting activities to identify advanced threats that evade automated detection. • Create and update incident response playbooks and standard operating procedures.

		• Generate and deliver reports on SOC activities, including incident trends and key performance metrics. • Stay informed about the latest cybersecurity threats, vulnerabilities, and best practices. • Provide input and recommendations for improving security controls and processes.
Support Audit and Risk activities	20%	This role shall be the focal point for all SOC reports from Audit and Risk teams.
System Security	20%	This role will conduct periodic review of systems within the Bank systems, to ensure that Bank systems are configured as per the Bank's Minimum Security Standard.

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, 2 weeks – 1 month, 1month – 3 months, 3-6 months, 6-12 months, above 1 year)*
6-12 months

Ideal Person Specifications
• A Bachelor's degree in Computer Science, Information Technology or related field. • Minimum 3 years working experience in a busy IT environment. • Certification in a systems security or audit related area, such as CEH, CISA, CISM or CISSP. • Have a deep interest in computing and cybersecurity • Excellent analytical, planning and organizing skills • Familiar with methods for ethical security hacking/penetration testing • Knowledge of SIEM toolsets • Experience / Knowledge on security Incident Detection and Response • Familiar with the tools and techniques used by hackers • Excellent written and oral communication skills

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