Job Title:	Senior Manager, Cybersecurity Operation	**Reports to:**	Head, Information Security
Department/ Sub-department:	Information Security	**Division:**	Information Security
Grade:	Band 6	**Date:**	
Job holder:		**Supervisor:**	
Signature:		**Signature:**	

Job Purpose Statement
The Cyber Security Operations Manager role is responsible for the continuous monitoring of technology assets for security incidents that impacts on confidentiality, integrity and availability of systems across the Bank. This role will drive the overall security monitoring and incident response program of the Bank, including implementation of policies and procedures on security monitoring and incident response, by putting in place the appropriate people, processes and technology. This role will also be responsible for security incident response, for effective response, containment and recovery from security incidents or breaches.

Key Results Areas		
Perspective	**% Weighting** *(to add up to 100%)*	**Output**
Security Monitoring	30%	• Primarily responsible for SOC Strategy, leading and managing a SOC team, ensuring that security incidents are correctly identified, analysed, defended, investigated, and reported, and cyber intelligence. • Monitor and analyse activity on networks, servers, endpoints, databases, applications, websites, and other systems, looking for anomalous activity that could be indicative of a security incident or compromise. • Ensure continuous integration of logs from technology assets into the SIEM to meet the security use cases and regulatory requirements. • Review of systems and network architecture and artefact configurations (Firewalls, Routers, Switches, IDS, IPS) and give practical recommendations.

		• Perform threat management & threat modelling, identify threat vectors and develop use cases for security monitoring. • Conduct threat, vulnerability and penetration testing on the Bank's environment on a periodic basis. Reporting the findings to stakeholders and advising on mitigation strategies. • Conduct Quality Assurance Programs, with regard to projects and system changes, to ensure that the bank is functioning at a high level of security, efficiency and effectiveness.
Cyber Incident Response	30%	• Manage the cyber incident response plan • Respond to incidents in accordance with the incident response plan • Effective communication and escalation during incident response. • Focal point of contact for cyber incidents. • Continuous improvement of the response plan
Information Security Policies & Procedures	20%	• Develop and maintain the required Information Security policies, procedures and standard operating procedures (SOPs) in relation to the SOC and incident response, to strengthen the current Security Operations. • Develop SOC performance management tools • Ensure compliance to SLA and process adherence to achieve operational objectives • Develop regular metrics, dashboards and reports on SOC operations for various stakeholders (Infosec Head, Senior Management, Regulators…)
Customer	10%	• Work closely and maintain a positive working relationship with internal teams and outsourced partners in the remediation actions of incidents within SLA • Direct and supervise the work of personnel and/or contractors assigned to the department. • Monitor and communicate cybersecurity incidents and track the remediation • Promote compliance culture within the Bank by providing guidance, training, consulting and coordinating cybersecurity compliance programs. • Ensuring proper and prompt service delivery

		• Maintaining effective communication with customers • Demonstrating appropriate attitudes towards consumers
Learning and growth	10%	• Responsible for delivering the performance objectives set and managing his/her own learning and development to build capacity and avail him/herself for coaching and training opportunities. • Achieve at least 50 hours of learning/training for both self and direct report through E-learning, Internal & External training activities. • Actively seek to learn, grow and stay abreast of current developments/trends in relevant technical/professional knowledge areas • Training and mentoring all bank staff around technology and cybersecurity aspects.

Job Dimensions

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

Stakeholder Management: key stakeholders that the position holder will need to liaise/work with to be successful in this role.	
Internal	**External**
Infosec Department IT Department ERM & Compliance Department Internal Audit	Managed Services partners External Auditors Regulators Forensic Experts

Decision Making Authority /Mandates/Constraints: the decisions the position holder is empowered to make *(Indicate if it is Operational, Managerial or Strategic)*.
Operational – Continuous Monitoring & Incident Response Managerial – Vendor management

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 Job Specifications
• Bachelor's Degree in, Information Security, Information Systems, Computer Science, Information Technology or related field required • 5+ years' Technical Experience in a busy IT Environment with good understanding of all fields of IT and an appreciation for emerging technologies • Relevant certifications in Information Security knowledge areas, such as security monitoring, threat intelligence, Information Security Management. • Experience in security device management, and in SIEM, IPS/IDS, DLP, Active Directory and other security technologies. • In-depth familiarity with security policies based on industry standards and best practices • Strong knowledge of technical infrastructure including operating systems, networks, databases, middleware etc., to address the threats against these technologies • Good knowledge of: End Point Security, Internet Policy Enforcement, Firewalls, Web Content Filtering, Database Activity Monitoring (DAM), Data Loss Prevention (DLP), Identity and Access Management (IAM) • Proficient in reports, dashboards and documentation preparation.

Technical Competencies	
	• Knowledge and experience in IT technology platforms across the IT domains. • Technical skills to effectively perform IS security management activities/tasks in a manner that consistently achieves established quality standards or benchmarks. • Knowledge and application of modern IS security management practices to proactively define and implement security quality improvements in line with technological and product changes. • Knowledge and effective application of all relevant banking policies, processes, procedures and guidelines to consistently achieve required compliance standards or benchmarks.

Behavioural Competencies	
	• 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