Job Title:	Manager, Cyber Security & BCM	**Reports to:**	Head, Information Technology
Department/ Sub-department:	Information Technology	**Division:**	Information Technology
Grade:	Band 5	**Date:**	
Job holder:		**Supervisor:**	
Signature:		**Signature:**	

Job Purpose Statement

The IT Security Manager role is responsible for continuous monitoring of technology assets for security assurance and incidents management and also to ensure the bank is protected against system failures by developing and supervising business continuity process for technology assets and systems. This is to ensure confidentiality, integrity and availability i of systems is maintained 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 and IT security training for effective response, containment and recovery from security incidents or breaches.

Key Results Areas

Perspective	**% Weighting** *(to add up to 100%)*	**Output**
Patch & Vulnerability Management and monitoring	20%	• Ensure all technology assets are maintained in the security management tools i.e. Vulnerability scanner, Ant Virus management tools, SIEM, patching tools, NAC, Asset register and Network Access Management tools • 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, this includes conducting venerability scans and review of various reports. • Review of systems and network architecture and artefact configurations (Firewalls, Routers,

		Switches, IDS, IPS) and give provide suggestions in improving controls. • This role will perform regular vulnerability assessments & penetration testing of systems, mobile applications and other IT assets across the NCBAT network, communicating and liaising with IT stakeholders on closure of the identified issues, in a prioritized manner. • 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. • Perform a critical role in reviewing audit reports and with system administrator support, to resolve identified audit related findings and recommend remediation actions.
Cyber Incident Response and Malware Management	20%	• 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 • This role will ensure that malware management practices and procedures are in place and executed efficiently. • Ensuring all endpoints and servers have anti-malware protection, regular review and remediation of malware threats detected and reporting on trends and statistics.
Information Security Policies & Procedures	20%	• Develop and maintain the required Information Security policies, procedures and standard operating procedures (SOPs) in relation to IT security matters. • Ensure compliance to SLA and process adherence to achieve operational objectives • Develop regular metrics, dashboards and reports on Head of Technology. • This role will develop and implement an effective information security awareness program covering all staff and stakeholders of the Bank.
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
Business Continuity Management Support and Risk Management	20%	• Work as a central point for business continuity tests by providing a leading role to all fail over tests including development of the Annual BCM test Plan. • Review test process and test results to improve fail over tests by identifying gaps and recommending resolution to the gaps • Support and ensure run books are reviewed, tested and documented for all systems • Review and ensure system are categorised as appropriate and all critical systems are provided with backup options at DR sites. • Ensure all systems are tested according to the Annual Plan and all results are properly documented as per policy • Ensure backup strategy and all necessary backup restore tests are conducted and tested as per policy to ensure data availability. • Manage closure of audit finding by doing follow ups of issues in teammate and ensure closure within defined time • Responsible for managing all technology risk related issues by working with system Administrators and log and track identified risks in the risks registers (GRC system). Also ensure the register as reviewed and reported on monthly basis.
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	Outsourced partners/Vendors

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
- Relevant certifications in Information Security knowledge areas, such as security monitoring, threat intelligence, Information Security Management.
- Experience in security device management and network devices, 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.
- Minimum 3-5 years working experience, with at least 3 years' experience in a busy IT security environment.

Ideal Job Specifications

- Certification in a systems audit or security related area, such as CEH, CISA, CISM or CISSP
- Experience in working with various vulnerability assessment & penetration testing tools.
- Experience in working in the IS function within a banking environment will be an advantage.
- Experience in audit of systems will be an advantage

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.
- Technical skills to effectively perform IT security management activities/tasks in a manner that consistently achieves established quality standards or benchmarks.
- Knowledge in penetration testing skills
- 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.

NCBAT Bank Core Value Behaviours (Performance Drivers)	
	• Driven: We are passionate, make bold decisions and learn from our failures. We seek new challenges and appreciate different views constantly raising the bar. We explore our full potential. • Open. Our interactions are candid, honest and transparent. We listen to each other and our clients. We are inclusive and always respect each other. • Responsive: We are proactive, act quickly and resolutely to deliver results. We put our customer's interests at the heart of all that we do. We keep it simple and seek new ways to improve. • Trusted: As a trusted partner we do what is morally right always. We keep our word. We are accountable and believe in each other. 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 •