Job Description

JOB TITLE	**IT Security Analyst**
LEVEL/BAND	**MM20**
DEPARTMENT	**Technology**
DIRECT REPORT (JOB TITLE)	**IT Security Operations Manager**

Overall Purpose of the Position

The IT Security Analyst role entails maintaining a secure enterprise environment to safeguard the Bank's sensitive information in line with regulatory requirements and industry-wide accepted information security principles. The individual shall work closely with other IT and business units to identify and correct flaws in the Bank's business solutions and underlying infrastructure, while implementing measures in order to continuously improve the Bank's overall IT security posture. This includes the support and monitoring of security control platforms, analysing security logs, events and other data to identify suspicious activity and alert on proactive risk mitigation approaches. The IT security analysts shall take an active role in supporting the IT operations team efforts in incident handling and counteracting potential breaches.

Operational Responsibilities

- To monitor, support and assist in the administration of the Bank's IT security platforms and associated controls;
- To contribute in the upgrades of existing IT security platforms and new implementation of IT security solutions;
- To actively monitor and analyse logs, events, and other data sources which will aid in the identification of suspicious activities and potential threats while triggering proactive risk mitigation approaches in line with industry best practices.
- To provide support services within the established service management procedures and SLA. Depending on the assigned incident, the IT Security Analyst may need to processes and resolve incidents and service requests. Such activities include but not limited to on-site and/or off-site investigation, devising workarounds and problem resolution;
- To participate in the change management requests review process from an IT security stand point;

- To assist in the preparation of service level agreements and standard operating procedures in relation to IT security operations in order to ensure that risks are maintained to an agreed acceptable levels and a high-level of service quality;
- To contribute in the development of IT Security operations policies, provide input during systems architecture review and produce documentation covering the Bank's IT Security posture;
- To assist in the implementation of patches and firmware upgrades on IT security equipment by following a low-risk approach.
- To maintain the Configuration Management Database for the IT security equipment in a comprehensive, accurate and timely fashion.
- To liaise with suppliers and service providers in order to acquire new IT solutions and services by following the established procurement procedures;
- To take ownership of the assigned projects' tasks and complete these to the expected quality and in a timely fashion;
- To contribute in gathering evidence, analyse findings and compiling the investigative reports related to security incidents in line with the Computer Security Incident response team guidelines and established policies.
- To conduct periodic vulnerability and penetration tests on the Bank's IT assets and the compilation of the associate findings and recommendations report and the subsequent follow ups on the agreed remedial actions;
- To assist in the development of disaster recovery test plans and executions;
- To provide support and housekeeping activities in relation to IT security operations;
- To liaise with other teams within the Bank in order to co-ordinate IT security operations activities;
- To conduct research on IT Security technologies in order to provide insight and input, aligned with the established guidelines, security policies and recommended industry standards, while compiling technical requirements and the review of blue prints;

General Responsibilities

- To submit any reports and/or lead any projects and activities as may be directed by the IT Security Operations Manager from time to time;
- To ensure compliance with Bank's policies, guidelines and underlying procedures at all times;
- To take an active role on committees and working groups and contribute accordingly;
- To participate in meetings when required and as directed by the Manager (IT Systems and Infrastructure) and take minutes accordingly;
- To ensure a high quality standard of work and service throughout;
- Willing to work on-call;
- To attend training as requested by the Bank;
- To perform any other duties that may be assigned to him/her from time to time.

Qualifications, Skills & Competencies

	SKILL	EXPERIENCE	QUALIFICATION
MANDATORY	Knowledge in IT technologies such as firewalls, network access control, IDS/IPS, operating systems (both Windows and Linux), IP Protocols, endpoint security and related system tools. Proficient in the use of network security toolkits; Familiarity with ISO 27001 standards. Good troubleshooting skills Possess good communication and report writing skills. Be a team player, reliable, and can work on his/her own initiative.	1 year working experience in a similar role within an enterprise environment administering security platforms Experience in Security Event Monitoring and log correlation using SIEM technologies Experience in Security incident investigations	Possess a Degree/IT Diploma in Computer Science or in Information security, or in a related field. Preferably has Industry specific certification such as CCNA Security and CISA
DESIRABLE			Ideally possess ITIL v3 skills.