v

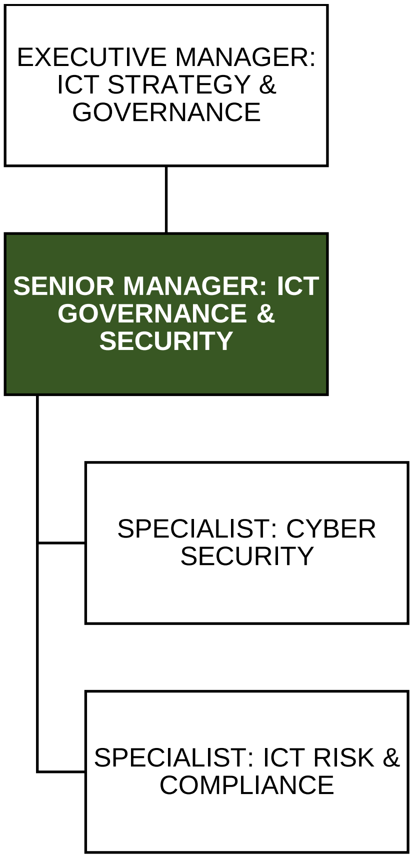
Job Profile

PROFILE INFORMATION			
JOB TITLE	**SENIOR MANAGER: ICT Governance & Security**		
JOB CLUSTER AND RANK	Management (Commandant)		
REGION/DIVISION	**ICT Strategy & Governance**		
LOCATION	Head Office		
MANAGER/SUPERVISOR	**Executive Manager: ICT Strategy & Governance**		
SUPERVISION	Specialist: Cyber Security Specialist: ICT Risk & Compliance		
PEER RELATIONSHIPS	OTHER MANAGERS		
GRADE		Grading Date	
LIAISON	**INTERNAL**	All Business Units	
	EXTERNAL	Stakeholders, Vendors	

PURPOSE STATEMENT

The Senior Manager: ICT Governance & Security is responsible for developing, implementing, and overseeing the information and communication technology (ICT) governance and security implementation within BMA. This role involves establishing and enforcing policies, standards, and procedures, implementation of IT and cyber security systems, tools and processes to ensure the confidentiality, integrity, and availability of BMA applications, data and systems.

ORGANOGRAM


EXECUTIVE MANAGER: ICT STRATEGY & GOVERNANCE
SENIOR MANAGER: ICT GOVERNANCE & SECURITY
SPECIALIST: CYBER SECURITY
SPECIALIST: ICT RISK & COMPLIANCE

DESCRIPTION

Key Performance Areas (KPAs)	Roles and Responsibilities	Weight %	Key Performance Indicators (KPIs)
ICT Governance Framework	• Develop and maintain the ICT governance framework, including policies, procedures, and standards. • Define and communicate the roles and responsibilities of key stakeholders in ICT governance. • Establish processes for the identification, assessment, and mitigation of ICT risks. • Prepare and present regular reports on ICT governance and security metrics to MANCO and relevant BMA committees.	**15%**	• Approved and updated Policies and Procedures • Audit Report • Risk Management Reports • Governance Committees Reports

Key Performance Areas (KPAs)	Roles and Responsibilities	Weight %	Key Performance Indicators (KPIs)
	• Monitor and report on compliance with ICT governance policies and standards. • Identify and communicate areas of improvement and recommendations to enhance ICT governance and security.		
Compliance and Risk Management	• Ensure compliance with relevant regulations, industry standards, and internal policies. • Conduct risk assessments and implement risk management strategies for ICT systems and processes. • Monitor and report on ICT compliance and ICT risk management activities to MANCO and relevant stakeholders	**15%**	• Prepare ICT Audit Report • Risk Management Reports
ICT Security Management	• Develop and implement ICT security policies, standards, and guidelines. • Conduct regular security assessments, vulnerability testing, and incident response planning. • Oversee the implementation of security controls, such as firewalls, encryption, and access controls. • Promote security awareness among employees and stakeholders through training and communication. • Manage and Monitor the Perimeter Security Management (Firewall Management, Web and E-mail Filtering) • Develop and deliver security training programs to enhance employees' understanding of security best practices. • Monitor and measure the effectiveness of security awareness and training initiatives. • Establish and manage an effective incident response plan for ICT security incidents. • Coordinate and lead incident response activities, including containment, investigation, and recovery. • Develop and maintain business continuity and disaster recovery plans for ICT systems.	**25%**	• Implemented Network Security. • Implemented End-user (endpoint) Security • Network Vulnerability. • Perimeter security. • IT Security Policy managed.

Key Performance Areas (KPAs)	Roles and Responsibilities	Weight %	Key Performance Indicators (KPIs)
	• Ensuring compliance to GITOC recommendations and achievement of GITOC (SCISS) strategic objectives in government. • Review violations of IT/IS Security policies and propose procedures to ensure violations are not repeated. • Perform due diligence assessments and contract reviews to ensure the security of outsourced services. • Monitor and enforce compliance with security requirements by vendors and third parties.		
Stakeholder Management and Relations	• Ensure the provision of effective and efficient ICT services and solutions to various departments within BMA to enable them to achieve their strategic objectives. • Coordinate and facilitate communication channels with internal and external key stakeholders to ensure proper messaging of ICT standards. • Implement and monitor Service Level Agreements with the relevant stakeholders. • Ensure that agreed service levels are consistently met on monthly basis. • Gather and disseminate accurate and timely information to all relevant stakeholders. • Ongoing management of strategic partners and vendors to ensure that they perform according to the SLA's. • Implementation of vendor scorecards to measure compliance with company expectations. • Conduct half-yearly reviews of strategic partners and vendor contracts to ensure SLA's are measurable and enable consistent delivery. • Ensure training of end users on any system or process changes.	**15%**	• ICT Customer Satisfaction Survey • Stakeholder Engagement Survey • ICT Contracts • Audit reports • Risk Management Reports
Financial Management	• Provide input in the planning and compilation of the business unit's annual budget aligned	**10%**	• Annual Operational Budget

Key Performance Areas (KPAs)	Roles and Responsibilities	Weight %	Key Performance Indicators (KPIs)
	to the operational plans to support the implementation of set objectives. • Ensure the effective implementation, management, and monitoring of the business unit's budget, and mitigate and report on any variances. • Monitoring financial control, budget management, and the procurement process to ensure compliance with the legislation e.g. (PFMA, PPFA, and BBBEE). • Ensure the deployment of proper financial controls to manage the business unit budget. • Report on and communicate any cost improvements and shortfalls.		• Variance Report • Budget Compliance Report
People Management	• Build and lead an effective and cohesive team through the effective management of divisional resources. • Drive the implementation of talent acquisition, succession planning, development, and retention strategies for the division. • Ensure the enhancement of relevant knowledge and skills through continuous coaching, mentoring and nurturing of talent in the business unit. • Create a high-performance culture and manage team performance effectively by translating and communicating the annual performance goals and measures into individual work plans based on agreed upon objectives. • Ensure the working environment contributes to improving employee engagement, recognition and increased productivity. • Ensure the management of poor performance and disciplinary matters in line with the BMA's policies and procedures.	**15%**	• All employees have revised up to date job profiles • Talent Management Plan • Timeous submission of performance agreements and reviews • % of staff in all training & development interventions • Employee Engagement Surveys • Timeous Resolution of disciplinary and Grievance procedures

CAREER PATH

Senior Manager: ICT Governance & Security	Executive Manager: ICT Strategy & Governance	

MINIMUM REQUIREMENTS/EXPERIENCE/KNOWLEDGE	
Minimum Qualifications	A Bachelor's degree in Computer Science, Information Technology, Information Systems and Management or an equivalent qualification. The following international certifications will serve as added benefits: CompTIA Security+, Certified Information Security Manager (CISM), COBIT 2019 Foundation, ITIL V4 Foundation.
Minimum Experience	• 8 to 10 years' experience, of which 5 should be in the management level.
Knowledge	• Risk & Compliance Monitoring • Compliance frameworks for Information Security, Compliance and IT Governance Standards • Border Management Authority Act,2020 • Minimum Information Security Standard (MISS) • ISO17799 or ISO27000 standard • Electronic Communication Act, Archiving Act and other related regulations • Router and Firewall Management • Filtering Applications • Cyber Security tools
Professional registration or license requirements	• None
Other requirements	• Flexibility in working hours will be required to meet demands of the role. • May be required to work overtime. • Valid driver's License

COMPETENCIES		
VALUES	**FUNCTIONAL**	**BEHAVIOURAL ATTRIBUTES (ENABLING)**
• Excellence • Integrity • Innovation • Patriotism • Professionalism • Teamwork and Collaboration • Vigilance	• IT Applications • IT Security • Writing Skills • Communication (Verbal and Written • Governance and Compliance • Research • Time management • Stakeholder Management and relations • Administration • Project Management	• Emotional Intelligence • Decision Making & Problem Solving • Resilience • Interpersonal Relations • Persuasion and influencing • Critical Thinking

	• Report Writing • Records Management • Information Management • Risk Management	

SYSTEM SKILLS	
Title	**Level**
ICT System Security	Intermediate