



Enterprise Technology & Security Manager

Status: Permanent

Location: Nelspruit

Grade: D4

Reporting line: Chief Information Officer (CIO)

Role Mandate

The Enterprise Technology and Security Manager provides strategic leadership for the organisation's technology direction, ensuring that ICT infrastructure, digital services, and technology governance effectively enable business objectives. With a strong focus on enterprise-wide security, this role is accountable for shaping and executing the enterprise technology strategy, embedding digital solutions into all operations, managing technology and cybersecurity risks, and ensuring the resilience, performance, and optimisation of all core ICT environments. The incumbent also guides the organisation's adoption of emerging technologies, ensuring they are integrated responsibly, securely, and in ways that enhance operational capability and long-term value. Through proactive planning, strong oversight, and continuous improvement, this role ensures a stable, scalable, and trusted technology foundation for the enterprise.

Key Accountabilities

Infrastructure & Technology Operations

- Provide strategic direction for the technology and security unit which includes enterprise architecture, networks, data centre and security competencies
- Oversee the design, implementation, and maintenance of enterprise ICT infrastructure (networks, servers, data centres, endpoints, and cloud environments)
- Ensure high availability, scalability, and performance of all ICT systems and services
- Lead the operational support of enterprise platforms, including incident, change, and problem management
- Manage technology & security budgets, lifecycle planning, and technology roadmaps
- Drive standardisation, automation, and optimisation across ICT operations
- Implement, maintain and improve communication systems, including electronic communication systems
- Conduct testing and analysis of all components of network and server infrastructure including the execution of the Disaster Recovery plan
- Stay abreast of new technological developments and assess these technologies in terms of the potential effect they could have on the productivity and efficiency of business currently and in future
- Create a strategy for establishing a secure and well managed enterprise environment in Azure, enabling Azure to become a critical part of the company's network. Use Azure services to meet resiliency requirements
- Provide in-house training as and when required.
- Interface with business unit managers to define infrastructure support initiatives & solutions for improving service efficiency and effectiveness
- Assist in the development of long-term strategic plans for the development of ICT requirements within business to ensure the infrastructure development is aligned to the strategy

Information & Cybersecurity

- Lead and coordinate cloud infrastructure projects from a technology architecture perspective, ensuring that infrastructure development activities are consistent with accepted best practices
- Plan, develop and lead the life cycle maintenance and replacement / upgrades of ICT Infrastructure at end of life
- Perform regular risk assessments, security audits, and control reviews to mitigate cyber risks. Ensure the monitoring, management and mitigation of infrastructure related risks
- Maintain the ICT risk register to ensure that risks are regularly reviewed, identified, assessed, reported and mitigated in line with recommended best practices
- Develop the architecture blueprint for the business, aligned with the ICT strategy
- Develop, implement, and monitor enterprise-wide information security strategies, policies, and standards
- Lead threat and vulnerability management, incident response, and cybersecurity awareness initiatives
- Ensure compliance with relevant legislation, regulatory requirements, and best practices (e.g., POPIA, ISO 27001, NIST)

Strategic Leadership & Governance

- Manage and build relationships with current and new infrastructure equipment and service providers according to business procurement policies
- Provide expert advice to the CIO and executive team on technology risks, investments, and security trends
- Collaborate with Application, Operations, and Digital teams to ensure secure, integrated technology delivery
- Develop and maintain business continuity and disaster recovery plans for critical infrastructure and services
- Contribute to ICT governance structures and reporting, including risk registers, audits, and board committees
- Monitor, maintain and improve an enterprise class ICT Infrastructure system based on the Microsoft platform and other industry leading systems over a large geographical area

People & Vendor Management

- Lead and mentor technical staff and contractors, building internal capability in infrastructure and cybersecurity
- Manage third-party service providers, technology partners, and outsourced contracts based on Service Level Agreements (SLA's)
- Foster a culture of accountability, resilience, and proactive security awareness within SAFCOL
- Build, lead, and govern the team by recruiting talent, maintaining a succession plan, regularly reviewing and updating role profiles to ensure clarity of accountability, and initiating and supporting disciplinary processes when required, including evidence collection

Minimum Requirements

- Bachelor's degree or equivalent (NQF 7) in Information Technology, Computer Science, Information Systems, or related field
- Relevant professional industry certifications in infrastructure, security, or architecture
- Advanced professional certifications aligned to the role's expanded strategic, security, and risk mandate, such as CRISC, CISM, CISSP, Cloud certifications (Azure, AWS, Google Cloud) - Preferred
- Platform based requirements: at least two (2) Certifications from below
 - Microsoft Certified: Azure Administrator Associate (AZ-104) – preferred
 - MCSA: Windows Server 2008 certification Minimum – preferred
 - Cisco CCNA or higher – preferred
- Experience in technology strategy development, enterprise architecture, or technology governance
- 7–10 years ICT experience, with at least 5 years in a senior infrastructure, security, or technology management role
- In-depth knowledge of networking technologies and concepts
- Experience with emerging technologies, digital transformation, or modernisation initiatives (cloud, AI, IoT, automation, etc.)
- In-depth knowledge of ICT security, data protection and knowledge of international information / cyber security standards promoted by NIST, ISACA, ISO
- Proven experience managing technology risk, business continuity, and ICT compliance frameworks (e.g., POPIA, ISO 27001)
- Managing hybrid infrastructure (on-prem, cloud, network)
- ICT Governance (King V, COBIT, ITIL, etc.)
- Experience with:
 - Dell Server and Storage units
 - Development & testing of Disaster Recovery plans
 - Patch management, Firewall Management & Backup Management
- Valid driver's license

Competencies

Leadership

- Strategic Thinking
- Leading Others
- Driving Change
- Operational Delivery
- Commercial Insight
- Self-Awareness

Behavioural

- Planning & Organising
- Analytical Thinking
- Problem Analysis & Solving
- Attention to Detail
- Influencing & Communication
- Regulatory & Compliance
- Stakeholder Management

Technical

- Infrastructure Administration
- Risk Management
- Project Management
- Security Infrastructure
- Networks

SAFCOL Group is an equal opportunity company with the focus on gender equality and people with disabilities.

Employment Equity will be taken into consideration in terms of all appointments within SAFCOL.

By submitting your CV to SAFCOL, you hereby give permission to circulate your information to the interview panel members for this vacancy only. Your information will not be used for any other role/purpose and will be disregarded after an offer has been made.

Interested qualified individuals can e-mail a concise CV and must submit relevant copies of qualifications in confidence to:

Ms. Sandra van der Walt, Human Capital Practitioner, sandrarecruitment@safcol.co.za (contact number 082 079 1092)

Closing Date: 5 February 2026

Should you not have received a response within 30 days of the closing date, please consider your application unsuccessful.