REFERENCE NR	:	**RE AD- VAC00986**
JOB TITLE	:	**Senior Manager: Security Operation Centre (SOC)**
JOB LEVEL	:	**D5**
SALARY	:	**R 638 491 – R 1 064 151**
REPORT TO	:	**Head of Department**
DIVISION	:	**Service Management**
Department	:	**Information System Security**
LOCATION	:	**SITA Centurion**
POSITION STATUS	:	**Permanent (Internal & External)**

Purpose of the job

To provide and manage information services including threat and risk management, architecture solution design, secure configuration, security operations (e.g. quality, change, incident, problem management, capacity planning, etc.), assurance and vulnerability management, governance and compliance, performance and service continuity management.

Key Responsibility Areas

- Create, execute and track a strategic, comprehensive enterprise information security and ICT risk management program which will place Information System Security as a strategic enabler to achieve the SITA security mandate
- Manage cyber and information security operations
- Manage ongoing information system security monitoring and regularly analyze information security risks by qualitative risk analysis to ensure compliance with security governance
- Manage and maintain relations with clients in line with the business goals and ensure that communication flow effectively
- Liaise with internal and external clients to identify and determine their security service requirements
- Financial and business management
- Human Capital Management.

Qualifications and Experience

Minimum: 3 – 4 year National Higher Diploma / National Degree in Computer Science or Information Technology or Network Management or a relevant discipline NQF level 7 qualification PLUS.

Certified information system security professional (CISSP) or Certified Information Security Management (CISM). Professional IT security management certification e.g ITIL Foundation, CoBit Foundation or GIAC, CCNP ,ISACA CRISC - security risk information and system control will be an advantage.

Experience : A minimum of 8-10 years practical ICT Security working experience which should include the following: 5 years experience in a leadership role in ICT environment such as architecture, operations, GRC (governance, risk

and compliance), including expertise in: At least 4 years as specialist / manager in information security environment such as governance, architecture, auditing, operations, policy and compliance. Working knowledge & experience of cloud security frameworks. Tool deployment and implementation experience on a global scale. Experience with virtualization and containerization (kubernetes, dockers). Experience with contract and vendor negotiations and management including managed services. Experience in preparing, managing operating budgets. Experience with business continuity, disaster recovery, risk management, vulnerability management, contract/vendor negotiations, and information incident management. Ability to engage and lead advisory committees. Experience with enterprise risk assessment methodologies. Experience in dealing with complex projects and meeting conflicting demands.

Technical Competencies Description

Knowledge of: Information security management frameworks, such as ISO/IEC 27001, and NIST.and security services (firewalls, proxy's, DNS, Mail relays etc.) Risk finance and risk control concepts. Enterprise risk management concepts, frameworks Deep understanding of operational integration of security functions. Strong knowledge of security, and network architecture. Deep knowledge of security best practices, principles, and common security frameworks. Excellent written and verbal communication skills and high level of personal integrity knowledge of the latest IT thinking and threat modelling methods together with a creative drive Analytical mind capable of managing numerous information sources and providing data analysis reports to senior management Strong customer focus – able to meet the demands of internal and external customers. Excellent communication skills –providing verbal and written communication Excellent Project management skills. Strong networking, consultation and negotiation

skills. Excellent Planning & organising. Financial management. Governance processes and standards (ISO 27001/ 27002, COBIT, ITIL). Proficiency in ICT technology securing and safeguarding (operating databases, applications, IS solutions). Knowledge of Cloud, Public Cloud security best practices and monitoring of systems and services hosted in the cloud (IaaS, SaaS etc.). Proficient in Microsoft products (Word, Excel, PowerPoint, Projects, and Vision). Technical competencies: Business Intelligence & Analytics, Financial Accounting, Human Capital Management

Information Security and Application Protection, IT Risk Management, Vendor/Supplier Management, Customer Experience, Collaboration, Communicating and Influencing, Outcomes driven, Innovation, Planning and Organising Creative Problem Solving, Managing People and Driving Performance, Decision-making, Responding to Change and Pressure, and Strategic Thinking.

Other Special Requirements
N/A

How to apply

Kindly send your CV to: Judith.recruitment@sita.co.za

Closing Date: 28 April 2021

Disclaimer

SITA is an Employment Equity employer and this position will be filled based on Employment Equity Plan. Correspondence will be limited to short listed candidates only. Preference will be given to members of designated groups.

- If you do not hear from us within two months of the closing date, please regard your application as unsuccessful.
- Applications received after the closing date will not be considered. Please clearly indicate the reference number of the position you are applying for.
- It is the applicant`s responsibility to have foreign qualifications evaluated by the South African Qualifications Authority (SAQA).
- Only candidates who meet the requirements should apply.
- SITA reserves a right not to make an appointment.

- Appointment is subject to getting a positive security clearance, the signing of a balance score card contract, verification of the applicant's documents (Qualifications), and reference checking.
- Correspondence will be entered to with shortlisted candidates only.
- CV`s from Recruitment Agencies will not be considered.
- CV's sent to incorrect email address will not be considered