REFERENCE NR	:	**VAC00434/24**
JOB TITLE	:	**Consultant Information System Security (Oracle Database Security)**
JOB LEVEL	:	**D2**
SALARY	:	**R 651 627 – R 977 440**
REPORT TO	:	**ISS Senior Manager**
DIVISION	:	**Service Management**
DEPT	:	**Information System Security**
LOCATION	:	**SITA Centurion**
POSITION STATUS	:	**3 years Fixed term contract** (**Internal & External**)

Purpose of the job

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

Key Responsibility Areas

- Design and implement security standards and procedures in systems and security policies and guidelines for all system security processes.

- Secures assets in the information system by defining and addressing possible and real security problems.

- Conduct, monitor and maintain threat and vulnerability assessments on a regular basis to minimize associated risk and improve the security capabilities within operational implementation, such as ICT infrastructure linked to SITA managed networks.

- Manage implementation of information security awareness and training programmes for employees and clients.

- Coordinate ongoing activities related to the development, implementation, and maintenance of information security controls and services aligned to the cyber security framework, policies, standards and procedures.

Qualifications and Experience

Required Qualification: 3-year National Diploma / Degree in Computer Science or Information Technology or Network Management or a relevant discipline NQF level 6 qualification.

Certification: Professional IT security management certification e.g. CISSP ITIL Foundation, CoBit Foundation or CISM, GIAC, CCNP, ISACA CRISC CCSP: Certified Cloud Security Professional Advanced certifications such as SANS GIAC/GCIA/GCIH, CISSP or CASP and/or SIEM specific training and certification will be an advantage. Certified information system security professional (CISSP) or Certified Information Security Management (CISM), would be an added advantage.

Experience: 6 - 7 years ICT Infrastructure or application development experience including IT Security working experience.

Technical Competencies Description

Knowledge of: System Engineering methods and Governance. Working knowledge of Enterprise architecture framework (TOGAF; Zachman; FEAF; MODAF; GWEA Framework; MIOS) Proven experience in working with Governance Processes and Standards (ISO 9001; ISO 27001/ 27002; ISO 12207 (SDLC); ISO 42010; COBIT; ITIL; UML). Knowledge of 7/10 CISSP domains Service Oriented Architecture (SOA). Working knowledge of Information System Security Technical Standards (e.g.: PKI, IAM, Cryptography). Exposure to ICT security architecture in a specific CISSP domain. Planning, designing and validating skills related to architecting security solutions. Detailed knowledge of the SOPs of the area/discipline the jobholder is works in (HR, Finance, IT, etc as well as how to apply it. ICT Policy and Strategy Management.

Other Special Requirements

(a) To be **certified and skilled** in the following Oracle Database Security components:
   (i) Key Vault and TDE Encryption;
   (ii) Audit Vault;
   (iii) Database Vault;
   (iv) Database Firewall; and
   (v) Data Masking.
(b) Resource requirements expected:
   (i) Oracle Database Administrator – Certified on 12c/19c; and
   (ii) Self-driven, taking ownership and security focused.
(c) High-Level tasks expected to be performed:
   (i) Taking ownership and responsibility for Database Security on the above components (a) from an operational perspective;
   (ii) Database Security fine tuning on all above components;
   (iii) Audit Vault and Database Firewall reporting;
   (iv) Internal/External auditor reporting;
   (v) Adding more environments as requested;
   (vi) Assisting end-customer DBAs in order to implement Database requests; and
   (vii) Analyse and resolve security issues.
(d) Focusing on Oracle Database Security with the following focus areas:
   (i) Oracle Database security administration;
   (ii) Administration of: Key Vault, Database Vault, Audit Vault and Database Firewall; and
   (iii) Oracle PL/SQL to assist with Audit Vault custom reporting.

How to apply

To apply please log onto the e-Government Portal: www.eservices.gov.za and follow the following process;

1. Register using your ID and personal information;
2. Use received one-time pin to complete the registration;
3. Log in using your username and password;
4. Click on "Employment & Labour;
5. Click on "Recruitment Citizen" to create profile, update profile, browse and apply for jobs;

Or, if candidate has registered on eservices portal, access www.eservices.gov.za, then follow the below steps:

1. Click on "Employment & Labour;
2. Click on "Recruitment Citizen"
3. Login using your username and password
4. Click on "Recruitment Citizen" to create profile, update profile, browse and apply for jobs

For queries/support contact egovsupport@sita.co.za OR call 080 1414 882

CV`s sent to the above email addresses will not be considered.

Closing Date: 31 March 2025

Disclaimer

SITA is an Employment Equity employer and this position will be filled based on Employment Equity Plan. Correspondence will be limited to shortlisted 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.