



VACANCY - 2050

| | | |
|------------------------|----------|---|
| REFERENCE NR | : | VAC00538/24 |
| JOB TITLE | : | Lead Consultant Information System Security (Technical Security Manager) |
| JOB LEVEL | : | D3 |
| SALARY | : | R 760 490 – R 1 140 736 |
| REPORT TO | : | Senior Manager Governance and Risk Management |
| DIVISION | : | Service Management |
| DEPT | : | Security Architecture and Development |
| LOCATION | : | SITA Centurion |
| POSITION STATUS | : | 3 years Fixed term contract (Internal & External) |

Purpose of the job

The role will be responsible for developing security system architecture design monitoring compliance with security governance, ensuring full alignment of risk management with business continuity, identifying cyber and information security management concepts to ensure the appropriate level of safety for all SITA and government infrastructure.

Key Responsibility Areas

- Create and maintain the system security framework to drive the Enterprise ICT security and risk management program and enable SITA to meet service requirements;
- Lead the implementation of information security awareness program and ensure the training and education of employees and clients;
- Work with all IT functional areas to design and support secure technologies to meet business /clients needs, build security controls and solutions according to approved architectural frameworks and standards ;
- Develops tactical response procedures for security incidents;
- Monitor compliance with security governance, ensure full integration of risk management with business continuity, both internally and externally, for recovery from disasters;
- Define cyber and information security management principles to initiate and define the security plan. Define principles for the cyber and information security management to initiate and define the security plan ;
- Ensure that all SITA and Government infrastructure has the correct level of protection to ensure secure operation.

Qualifications and Experience

Minimum: 4-year National Diploma / National Degree in Computer Science or Information Technology or Network Management or a relevant discipline NQF level 6 qualification PLUS Certified information system security professional (CISSP) or Certified Information Security Management (CISM) Professional IT security management certification e.g CISSP ITIL Foundation, CoBit Foundation or CISM, GIAC, CCNP, ISACA CRISC\$ security risk information and system control will be an advantage. Membership to a (ISC)2 an ISACA and professional body will be an advantage.

Experience: 7 - 8 years practical experience in Information and Communication Technology (ICT) Infrastructure or Information Security (IS) or application life cycle management.

Technical Competencies Description

Working knowledge of Information technology security risk management. Exposure to enterprise architecture frameworks (e.g. TOGAF GWEA MIOS). knowledge of governance processes and standards (e.g. ISO 27001/ 27002 COBIT ITIL). Exposure to information system security technical standards (e.g.: SSL certificates, anti-virus protection, etc.) Experienced in (e.g. Service Management, Converge Communication, Risk Management, Information Technology, Applications, etc.

Skills: Customer Relationship Management; Database Administration; Information Management; Information Security and Application Protection; IT Project Management; IT Service Management; IT Risk Management.

Leadership Competencies: Customer Experience; Collaboration; Communicating and Influencing; Honesty, Integrity and Fairness; Outcomes driven; Innovation; Planning and Organising; Creative Problem Solving; Managing People and Driving Performance; Decision-making; Responding to Change and Pressure; Strategic Thinking.

Interpersonal/behavioural competencies: Active listening; Attention to Detail; Analytical thinking; Continuous Learning; Disciplined; Resilience; and Stress Management.

Other Special Requirements

Provisioning of Technical Security Manager is to:

- Lead and manage a team of SITA client security support resources, providing technical guidance, mentorship, and support;
- Develop and implement security strategies, policies, processes, procedures and standards aligned with industry best practices and regulatory requirements;
- Conduct regular security assessments and audits of systems, networks, and applications to identify vulnerabilities and risks;
- Design and implement various security controls and solutions to protect the SITA client environment;
- Monitor security infrastructure and systems for security incidents, investigate breaches, and implement incident response procedures as necessary;
- Collaborate with SITA client and SITA IT teams and stakeholders to integrate security requirements into systems development lifecycle (SDLC) processes and infrastructure projects.
- Stay current with emerging threats, vulnerabilities, and cybersecurity trends, and continuously update security measures and practices; and
- Prepare and present security reports, metrics, and recommendations to SITA client senior management and stakeholders.

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: 02 December 2024

Disclaimer

SITA is Employment Equity employer and this position will be filled based on Employment Equity Plan. Correspondence will be limited to short listed candidates only.

- 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 applicants' documents (Qualifications), and reference checking.
- Correspondence will be entered to with shortlisted candidates only.
- CV's from Recruitment Agencies will not be accepted