



VACANCY

REFERENCE NO	:	VAC07820
JOB TITLE	:	Advance Cloud Architect (Security)
JOB LEVEL	:	D4
SALARY	:	R 715,548 - R 1,192,580
REPORTS TO	:	Enterprise Architect
DIVISION	:	IT Infrastructure: Hosting
Department	:	Technology, Strategy and Planning: Architecture
LOCATION	:	SITA Centurion; Pretoria
POSITION STATUS	:	Permanent (Internal /External)

Purpose of the job

The role is responsible for the design, development, engineering and implementation of cloud security architectures, processes and initiatives for cloud services that fulfil legislative obligations and data protection requirements and ensure alignment with the Government and Corporate security acts, policies, and strategies.

Key Responsibility Areas

- Develop and design cloud security architecture strategies, frameworks and reference models.
- Provide the project teams with technical leadership on cloud security projects / solutions and implementations.
- Identify, assess, monitor and evaluate technical and cyber security risks for cloud solutions.
- Collaborate with all IT functional areas to design and support secure technologies to meet business needs, build security controls and solutions for cloud technology in accordance with approved architecture frameworks and standards.
- Develops tactical response procedures for security incidents.

Qualifications and Experience

Minimum Qualifications: National Diploma in IT /Bachelor's Degree in Computer Science, Information Systems/Engineering or Relevant equivalent to NQF Level 6 plus Professional certification such as CCSP, Security certification, ISC2, CISSP, CISM, CISA CCNE, Cloud certification, Cloud Security certifications, Cloud Platform and Infrastructure etc. is strongly preferred
Professional certification such as CCSP, AWS security certification, ISC2, CISSP, CISM, CISA, CCNE, Cloud certification, Cloud Security certifications, Cloud Platform and Infrastructure etc. is strongly preferred.

Experience: 9-10 years ICT experience in a large corporate/Public sector Organization which should include:

- Experience as a technical lead and architect for security
- Strong experience with security technologies
- Hands-on experience with one or more major cloud technologies.

- Experience in deploying and securing cloud platforms.
- Experience in cloud security compliance.
- Experience in Cybersecurity, Distributed-Denial-of-Service Attacks, Shared Cloud Computing Services, Data Loss, Phishing and Social Engineering Attacks, Crypto jacking, etc.
- Experience in design, implementation and operation of large-scale security architecture solutions in a large and complex multi-supplier / multi-platform environment.
- Experience in designing, implementing, and testing cloud security controls.
- Experience integrating and migrating legacy platforms and applications with cloud-based systems strongly preferred.

Technical Competencies Description

Knowledge of: Deep understanding of cloud architecture. 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; Extensive knowledge of systems architecture; Deep working knowledge of cloud security frameworks; Good knowledge and understanding of risk management processes and experience in conducting risk assessments; Good knowledge and understanding of business continuity and disaster recovery; Deep understanding of security management solutions; Extensive knowledge of developing and documenting security architecture and plans, including strategic, tactical and project; Strong organizational and project management skills; Thorough understanding of Information Security frameworks and good practices and ability to strike a balance between an academic and pragmatic approach; Extensive knowledge of security issues, techniques and implications across all existing computer platforms; Excellent communication and presentation skills (written and verbal). Ability to create, maintain and organize documentation to support architectural standards and principles; Strong project management skills, with a high aptitude in managing multiple projects; Ability to negotiate with multiple stakeholders; Good Knowledge of infrastructure, key processes, and technology oriented risk issues, specifically around security and privacy; Excellent analytical, decision-making, and problem-solving skills as well as project management; Outstanding presentation and persuasion capabilities that elicit confidence and credibility.

Other Special Requirements

- Ability to translate complex technical concepts effectively to help customers understand their technological needs
- Ability to build consensus, build followership with business line owners
- Ability to develop effective partnerships with senior management and peer organizations
- Ability to drive change set priorities, drive performance, and execute plans on schedule within a defined multifaceted structure
- Ability to appropriately exert influence to drive priorities and achieve results
- Ability to define plans and execute roadmaps
- Ability to formulate security architecture vision and translate vision into execution
- Ability to manage across functional teams, influence others to accomplish set goals, and organize resources
- Ability to develop partnership-oriented relationships with business executives and functional leaders, especially as it relates to operations and technology

- Ability to effectively influence senior level management and key stakeholder and Ability to develop effective working relationship and work collaboratively across various technical and business units

How to apply

Kindly forward your CV to: Lerato.recruitment@sita.co.za stating the position applying for and the relevant reference number

Closing Date: 17 June 2020

Disclaimer

SITA is an Employment Equity employer and these positions will be filled based on Employment Equity Plan. 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 the right not to make an appointment;
- Appointment is subject to getting a positive security clearance, the signing of a contract of employment verification of the applicant's documents (Qualifications) and reference checking;
- Correspondence will be entered into with shortlisted candidates only.