PARLIAMENT
OF THE REPUBLIC OF SOUTH AFRICA

PO Box 15 Cape Town 8000 Republic of South Africa
Tel: 27 (21) 403 2911
www.parliament.gov.za

JOB DESCRIPTION

ORGANISATION	Parliament of the R.S.A
DIVISION	Information and Communication Technology
JOB TITLE	ICT Governance and Security Specialist
RESPONSIBILITY OF JOB	The successful candidate will be responsible for ensuring, ICT governance by monitoring, evaluating and reporting on legal, industry best practices, and policy compliance for ICT and provide guidance on security on infrastructure and applications platforms.

ORGANISATION CHART (JOB TITLES ONLY)

1 ST LEVEL SUPERIOR	**Chief Information Officer**
THIS POST	**ICT Governance and Security Specialist**

SUBORDINATES [TITLES]	**NO.S**
None	0

QUALIFICATIONS (MINIMUM)	
SCHOOL	Grade 12 or NQF Level 4
POST SCHOOL	BSc IT or B Com IT or National Diploma
STATUTORY REQUIREMENT	None

MINIMUM EXPERIENCE (TYPE & PERIOD – THIS AND/OR OTHER JOBS):

5 to 8 Years Relevant Experience

IMPORTANT CONTACTS WITHIN ORGANISATION	**IMPORTANT CONTACTS OUTSIDE ORGANISATION**
• Members of Parliament • Parliamentary Staff	• Service Providers

Job Description Verified By Line	**Ms U Mtya**
Job Description Updated By	**Mr R Buthelezi**
Job Description Authorized By DM:	**Ms U Mtya**
Job Description Approved By HR Executive	**Mr L Makele**
Date Of Approval	
Job Grade	**D1**

PARLIAMENT
OF THE REPUBLIC OF SOUTH AFRICA

PO Box 15 Cape Town 8000 Republic of South Africa
Tel: 27 (21) 403 2911
www.parliament.gov.za

JOB DESCRIPTION SUMMARY	
JOB TITLE	ICT Governance and Security Specialist
RESPONSIBILITY OF JOB	The successful candidate will be responsible for ensuring, ICT governance by monitoring, evaluating and reporting on legal, industry best practices, and policy compliance for ICT and provide guidance on security on infrastructure and applications platforms.
KEY PERFORMANCE AREA	1. ICT Governance Compliance 2. ICT Policy and Processes 3. ICT Governance Auditing and Risk Management 4. ICT Security competence Infrastructure and applications platforms
SPECIAL REQUIREMENTS	• ITIL - ITSM (IT Service Management) 6 years • COBIT (procedures, processes) • COBIT and /or ITIL /ISO 27002 Training and Certification • Security certifications, such as CISM / CISSP, Microsoft Certified Systems engineer will be an added advantage • ICT governance and security with emphasis on experience in Patch Management, anti-virus and vulnerability management • Experience in developing & implementing ICT Disaster Recovery Plans – will be an taken into account OBIT (procedures, processes) • Policy development • Information Security Standards • Project Management – PMBOK ,Prince2 • Risk Management

PO Box 15 Cape Town 8000 Republic of South Africa
Tel: 27 (21) 403 2911
www.parliament.gov.za

	• Strong Organizing and Planning skills • Negotiation skills • Good oral and written communication skills • Customer oriented approach, dependable, ethical, professional, team player • Advanced IT literacy • Sound communication skills • Sound interpersonal skills • Ability to work under pressure • Ability to exercise discretion
COMMENTS	Highly desirable certifications for information security not part of the Minimum requirements: • Comp TIA –Security + • (ISC) – Certified Information Systems Security Professional (CISSP) • ISACA – Certified Information Systems Auditor (CISA)

PO Box 15 Cape Town 8000 Republic of South Africa
Tel: 27 (21) 403 2911
www.parliament.gov.za

JOB CONTENT	
KEY PERFORMANCE AREA (WHAT)	**ACTIONS (HOW)**
1. ICT Governance Compliance	• Provide guidance relating to the compliance for ICT Asset Management, legal ,procedural issues, policies, and service support and service delivery • Compile and maintain an effective compliance and governance framework for ICT • Ensure ICT compliance and governance Issues/concerns within Parliament are appropriately evaluated, investigated and resolved • Identify potential areas of non-compliance and governance vulnerability and risk • Develop and implement corrective action plans for resolution of compliance problematic issues • Provide general guidance on how to avoid or deal with governance compliance issues for new projects • Ensure support for all aspects of ICT governance and compliance across a variety of platforms, technologies and disciplines • Ensure alignment to COBIT(Control Objects for Information Related Technology), ITIL (Information Technology Infrastructure Library) framework and Security Framework ISO 27002 • Ensure that Policies, Service Support, Asset Management, and Legislative issues are

PO Box 15 Cape Town 8000 Republic of South Africa
Tel: 27 (21) 403 2911
www.parliament.gov.za

	aligned to the core objectives over the Medium Term Expenditure Period
2. ICT Policy and Processes	• Develops, initiates and revises processes and procedures for Service Support and Asset Management • Assess and develop ICT polices • Promote awareness and facilitates marketing of new policies and processes. • Enhances and align to best practices for policies and processes. • Ensure alignment to COBIT(Control Objects for Information Related Technology), ITIL (Information Technology Infrastructure Library) framework and Security Framework ISO 27002
3. ICT Governance Auditing and Risk Management	• Review and audit ICT compliance • Assess ICT policies, processes and Legal compliance procedures. • Develop recommendations for non-compliance and or risk related areas • Review ICT policies, processes and legal procedures to ensure alignment to Minimum Information and Security Standards and Minimum interoperability standards. • Assess alignment to COBIT(Control Objects for Information Related Technology), ITIL (Information Technology Infrastructure Library) framework, Security Framework ISO 27002 • Perform risk analysis and provide mitigating recommendations

PO Box 15 Cape Town 8000 Republic of South Africa
Tel: 27 (21) 403 2911
www.parliament.gov.za

4. ICT Security competence Infrastructure and applications platforms	• Provides guidance on security on infrastructure and applications platforms • Identify security weaknesses • Create and maintain the enterprise's security documents (policies, standards, and procedures) and ensure compliance; security architecture design and implementation plan and security awareness campaigns and perform training on key security aspects and process change; • Review of system implementation, project management activities, change control audits and data center security; • Prioritize specific security solutions