Job and Person Specification

Title of Role: Cyber Security & Risk Adviser

Business Unit: Technology Services

Division: Projects and Technology

Remuneration Level: ASO5

Type of Appointment: Term

Position Number: P44775

Job and Person Specification Approval

……...../……../…….. DELEGATE

Primary Purpose

The primary purpose of the Cyber Security & Risk Adviser is to successfully coordinate elements of the Department's Cyber Security and Risk Program, primarily in the areas of cyber risk management, cyber security awareness, information classification, governance, compliance, vulnerability management and South Australian Cyber Security Framework (SACSF) compliance.

The position is also required to undertake responsibility for work related to a range of discreet security projects as part of the implementation of the SACSF and the AGD Cyber Security and Risk Strategy.

The Cyber Security & Risk Adviser is also required to provide security advice to business unit initiatives.

Reporting Relationships

- Reports to the Manager, Cyber Security and Risk.

Key Relationships/Interactions

- Technology Services
- Cyber Security and Information Technology Teams
- Employees and executives across AGD
- Other Government agencies
- External ICT providers

Key Challenges

- Supporting cultural change across complex and diverse business units.
- Communicating benefits of cyber security to broader management groups within the Department.

Special Employment Conditions (if relevant)

- Some out of hours work may be required at periods of high demand
- Occasional interstate and intrastate travel may be required

Government of South Australia
Attorney-General's Department

AGD Conditions

- Participation in quarterly performance review and development;
- Actively participate in all mandatory training requirements;
- Abide by the standards in the Code of Ethics for the South Australian Public Sector (the Code), relevant legislation and AGD policies and procedures; and
- Employment is dependent upon a National Police Certificate clearance that the AGD finds satisfactory.
- Appointment to this role is subject to Periodic Criminal History and other Background Screening that AGD finds satisfactory. The incumbent must participate in criminal history (Police Records Checks) on a periodic basis and be eligible to obtain an Australian Government Security Clearance to the level of Protected (Baseline).

Flexible Working Arrangement Options

- Flexitime
- Part-time
- Compressed weeks

Responsibilities

This Job and Person Specification provides an indication of the type of duties you will be engaged to perform. You may be lawfully directed to perform any duties that a person with your qualifications, skills and abilities would reasonably be expected to perform. The Cyber Security & Risk Adviser is responsible for:

Key Responsibilities	Specified Duties	Performance Indicator/Measurement
Cyber Security & Risk Program Implementation	• Planning and coordinating department-wide projects incorporating the requirements for the SA Cyber Security Management Framework (SACSF). • Contribute to business cases and consult on and implement policies in support of the Risk and Cyber Security Program with particular emphasis on the requirements of the SACSF. • Provide advice and consultancy on existing and emerging cyber security trends and threats impacting business operations.	• Business units are informed and aware of cyber security risks and controls. • Controls are in place for identified cyber security risks. • Security initiatives meet whole of government mandated requirements.
Project management and Implementation	• Coordinate Cyber Security and Risk projects, including SACSF initiatives and the implementation of the Information Security Management System, in accordance with internal project management frameworks and practices. • Ensure a clear focus on the successful delivery of outcomes at all times. • Develop strategies to ensure security solutions and controls are implemented correctly. • Coordinate risk management and assurance processes. • Develop and maintain project management plans and associated documentation including forecasting and reporting. • Review and record project progress, issues and outcomes, communicating to management in a timely manner. • Monitor and manage project budgets and expenditure. • Determine quality requirements and implement quality assurance.	• Projects completed on time and within agreed scope. • Projects implemented according to AGD policy and frameworks. • Risks and issues identified and managed for projects in accordance with policy and process. • Appropriate project documentation developed and maintained throughout projects. • Project plans and reports provided as required. • Budgets monitored and tracked as required. • Projects finalised and closed in accordance with departmental procedures. • Quality assurance requirements implemented and adhered to.
Communication and Relationship Building	• Establish and maintain open and effective working relationships with management and stakeholders to ensure initiatives are coordinated and milestones are achieved. • Manage stakeholder expectations.	• Stakeholders consulted where appropriate with regard to delivery of outcomes.

Contribute to Culture	• Actively participate and contribute to responsible and safe work practices; • Embrace diversity and cultural differences in the workplace.	• Work practices are safe and Work Health and Safety legislation, policies and procedures are adhered; • Respectful behaviour observed when faced with diversity/differences in opinion.
Compliance	• Responsible and accountable for adhering to the requirements of the WHS Act 2012; relevant WHS Regulations 2012; the Equal Opportunity Act 1984; the PS Act 2009; the Code of Ethics for Public Sector employees; the principles of diversity; and the Department's policies and procedures. • Keep accurate and complete records of business activities in accordance with the State Records Act 1997.	• Abides by the Acts, Regulations, Policies and Procedures relevant to employees of the Department. • Documents and correspondence filed according to States Records Act, 1997.

Technical Expertise

Technical Expertise (Essential)	• Successful experience in the delivery of projects, programs or business initiatives. • Experience in developing controls for identified risks and in communicating the requirements to the business. • Well-developed written and verbal communication skills in particular the demonstrated ability to provide sound advice and prepare written reports and briefings to stakeholders. • Demonstrated ability to effectively contribute to the management of incidents of a cyber security nature. • Understanding of audit processes and procedures. • Experience in developing and implementing information classification and cyber security awareness materials and policies. • Knowledge of the SA Cyber Security Framework (SACSF). • Understanding of the cyber security threat landscape. • Experience in the implementation of innovative security solutions and controls. • Demonstrated knowledge of contemporary ICT security practice.
Technical Expertise (Desirable)	• Knowledge and experience in implementing an Information Management System in accordance with ISO/IEC 27001. • At least 2 years' experience in a risk and cyber security related role. • Knowledge of government processes and proven ability to deliver timely, high quality outcomes within government frameworks. • Knowledge of ICT principles and use within a large diverse organisation.
Qualifications (Desirable)	• Certified Information Systems Security Professional (CISSP) and/or Certified Information Security Manager (CISM). • Certified Risk and Information Systems Control (CRISC).
Skills Framework for the Information Age (Essential)	• **Information Security**. Develops and communicates corporate information security policy, standards and guidelines. Ensures architectural principles are applied during design to reduce risk. Drives adoption and adherence to policy,

	standards and guidelines. Contributes to the development of organisational strategies that address information control requirements. Identifies and monitors environmental and market trends and proactively assesses impact on business strategies, benefits and risks. Leads the provision of authoritative advice and guidance on the requirements for security controls in collaboration with subject matter experts. • **Information Assurance**. Develops information assurance policy, standards and guidelines. Contributes to the development of organisational strategies that address the evolving business risk and information control requirements. Drives adoption of and adherence to policies and standards. Ensures that architectural principles are followed, requirements are defined and rigorous security testing is applied. Ensures that accreditation processes support and enable organisational objectives. Monitors environmental and market trends and assesses any impact on organisational strategies, benefits and risks. • **Business Risk Management.** Plans and implements complex and substantial risk management activities within a specific function, technical area, project or programme. Implements consistent and reliable risk management processes and reporting to key stakeholders. Engages specialists and domain experts as necessary. Advises on the organisation's approach to risk management. • **Consultancy.** Takes responsibility for understanding client requirements, collecting data, delivering analysis and problem resolution. Identifies, evaluates and recommends options. Collaborates with, and facilitates stakeholder groups, as part of formal or informal consultancy agreements. Seeks to fully address client needs and implement solutions if required. Enhances the capabilities and effectiveness of clients, by ensuring that proposed solutions are properly understood and appropriately exploited.

Behavioural Capabilities

The AGD Performance Matrix describes the behaviours expected of AGD employees across various levels in the Department.

Descriptors below detail the behavioural capabilities required for performance in Cyber Security and Risk Adviser role. KEY behaviours for this role are listed with the critical behaviours highlighted in **bold**. This broader group of behaviours are applicable to your ongoing success in the role.

Elements	Behaviours
Supports Strategic Direction	• Communicates plans in practical terms to others • Identifies and manages risk as appropriate and escalates as necessary • **Adopts and manages a balanced approach to risk aversion and risk taking** • Contributes to the drive for change and innovation • **Promotes creative and innovative thinking**
Achieves and Monitors Own Results	• Critically evaluates issues and ensures solutions are practical and achievable • **Develops plans with clear outcomes and supports others to achieve these** • **Negotiates as necessary to achieve outcomes** • Takes responsibility for the delivery of quality and timely results • Measures performance and acts on opportunities for continuous improvement
Supports Service Delivery Excellence	• Uses capability and expertise of the workgroup to achieve outcomes • **Effectively manages and coordinates resources for optimal outcomes.** • Identifies and delivers high quality internal and external customer service • **Sets clear performance standards that are linked to business unit outcomes.** • Translates performance requirements into achievable outcomes
Fosters Working Relationships	• Collaborates with relevant stakeholders • **Develops effective working relationships and internal and external networks** • **Makes an effort to understand others' perspectives, motives, agenda** • Openly shares information and knowledge as appropriate • **Tailors approach and communication style to suit the situation and audience**
Supports Personal Drive and Professionalism	• Demonstrates respect for others and high ethical standards • **Demonstrates and promotes professionalism and confidentiality** • Remains positive and recovers quickly from setbacks • **Displays flexibility and adaptability** • Ensures a focus on wellbeing for self and others and raises concerns where necessary

Acknowledged by occupant			/ /
	---------- (Print name)	---------- (Signature)	----------
Acknowledged by line manager			/ /
	---------- (Print name)	---------- (Signature & title)	----------