Role description

Role information

Role title	Manager, Cyber Security, Change and Problem Governance
Classification	ASO8
Agency	Department of the Premier and Cabinet (DPC)
Division	Chief Operating Officer
Business unit	ICT and Business Services
Reports to	Head of Digital and Business Technology
Roles reporting to this role	• Cyber Compliance and Governance Specialist • Cyber Security Technical Specialist • Cyber, Change, Compliance and Problem Officer(s)

Role purpose

The Manager, Cyber Security, Change and Problem Governance is responsible for the oversight of cyber security, ICT change and problem management and governance to support the delivery of secure, resilient, and trusted ICT services for DPC and its attached offices.

Key responsibilities

1. Lead, develop and manage the multidisciplinary Cyber Security, Change and Problem Governance team, setting priorities, managing performance and building capability
2. Provide authoritative cyber security governance, risk and compliance advice across projects, procurement, architecture, operations and service delivery, ensuring alignment with organisational and government policies, standards and regulatory requirements
3. Coordinate cyber crisis, emergency management and resilience activities, including supporting the Head of Digital and Business Technology through advice, documentation, reporting and incident management support
4. Lead the management and continual improvement of the Information Security Management System (ISMS) including governance frameworks, procedures, evidence repositories, control ownership and reporting
5. Manage ICT change governance processes so that changes are assessed for security impact, risk, readiness, approvals, implementation quality and post implementation outcomes

6. Lead incident, vulnerability, investigation and problem management activities, ensuring effective response coordination, escalation, root-cause analysis, remediation and continual improvement of operational resilience
7. Monitor and report on cyber security, change and problem governance performance, and provide timely input to the Risk and Audit function to support enterprise risk and audit oversight.

Key relationships

- **Head of Digital and Business Technology:** Provide strategic advice, reporting and recommendations on cyber security, change management, problem management and ICT risk.
- **Cyber Security, Change and Problem Governance Team:** Lead and enable delivery through clear communication, setting direction and ensuring alignment.
- **DPC ICT leadership team and Business Services teams:** Work closely to promote alignment, information sharing and continuous improvement.
- **Risk and Audit team:** Support risk management and audit activities through the provision of information, advice and reporting.
- **Business unit leaders and staff**: Partner to understand priorities, shape solutions, and ensure responsive service delivery.
- **ICT leaders across SA Government**: Collaborate to align with whole-of-government strategies, standards, and shared initiatives.
- **Office of the Chief Information Officer (OCIO):** Engage to meet policy, security, and compliance obligations.
- **Vendors and strategic partners:** Oversee supplier relationships, ensuring performance, value for money, and delivery of strategic outcomes.
- **Cross-Government committees and forums:** Represent DPC and influence sector-wide ICT strategy, standards, and innovation initiatives.

Special conditions

- The successful applicant will be required to undergo a Nationally Coordinated Criminal History Check (NCCHC) in accordance with departmental policy.
- The successful applicant will be required to obtain and maintain a Security Clearance at Negative Vetting level 1.
- The employee is required to participate in the department's Performance Development Program
- The employee may be assigned to another position at this remuneration level or an equivalent classification within DPC.

- Some out-of-hours work may be required, including participation in incident response or critical service restoration activities.

Selection criteria

The selection criteria are a combination of any role specific criteria (where applicable) and focus capabilities selected from the DPC Capability Framework.

ROLE SPECIFIC CRITERIA

1. Demonstrated experience managing cyber security, ICT change, incident, vulnerability and problem management processes, Information Security Management Systems (ISMS), cyber security risk management, security assurance, and the application of relevant frameworks, standards and government policies.

2. Relevant tertiary qualification in information technology, cyber security, governance, risk management, audit, service management or a related discipline, and/or equivalent experience and recognised industry certifications (e.g. CISSP, CISM, CRISC, ISO 27001 Lead Implementer or Lead Auditor).

DPC Capability Framework



The DPC Capability Framework outlines the knowledge, skills and abilities required to perform a role successfully. It groups capabilities into five core areas:

- Personal Attributes
- Relationships
- Results
- Business Enablers
- People Management (only relates to roles with leadership responsibilities)

The focus capabilities are most critical to successful performance in this role and are assessed during the recruitment process along with any role specific criteria set out above. The focus capabilities for this role are listed below, each with a brief description and examples of the behaviours expected at the required level.

FOCUS CAPABILITIES			
GROUP	**CAPABILITY**	**BEHAVIOURAL INDICATORS**	**LEVEL**
Personal Attributes	**Demonstrate Courage, Resilience and Adaptability** Be willing to embrace change and remain focused in challenging situations.	Ability to: • Demonstrate flexibility and initiative, adjusting your approach quickly and confidently when situations change • Provide clear, honest feedback and practical advice to support effective outcomes • Consider ideas that are challenged, take time to understand the reasoning behind the challenge and respond in a balanced, constructive way • Address difficult issues directly, working through them thoughtfully and exploring alternative options where needed • Maintain professionalism under pressure and apply effective strategies to navigate and manage demanding or complex situations	Proficient
Relationships	**Communicate Effectively** Communicate clearly, pay attention to others and respond constructively.	Ability to: • Adapt your communication style to suit diverse audiences and remove barriers that may limit participation • Clearly explain complex concepts and arguments to individuals and groups • Create opportunities for others to be understood and encourage them to express their perspectives • Share information across teams and business units to enable informed decision making • Utilise a range of styles and formats to suit the intended audience • Use effective communication channels to share information, engage and interact with a broad range of audiences	Proficient
	Influence and Negotiate Gain consensus, secure commitment from others and resolve issues and conflicts to drive positive outcomes for all stakeholders.	Ability to: • Use facts, knowledge and experience to support recommendations and strengthen arguments • Strive to reach outcomes that are constructive and satisfactory for everyone involved • Identify and resolve issues in collaboration with other employees and stakeholders	Proficient
Results	**Deliver results** Achieve results through a focus on quality outcomes and efficient use of resources.	Ability to: • Leverage own and others' expertise to achieve desired outcomes, and take responsibility for delivering intended outcomes • Clearly communicate expected goals and recognise employee success in achieving objectives • Ensure others understand expected goals and actively recognise their achievements in meeting these objectives • Determine the resources needed and deliver outcomes on time and within budget • Use data-driven insights to evaluate outcomes and shape continuous improvement initiatives • Identify shifting priorities and ensure the allocation of resources meets new business needs • Ensure financial impacts of changing priorities are thoroughly assessed and incorporated into budget planning	Proficient

Results	**Think Through and Solve Problems** Solve problems by assessing the broader context, challenge inefficiencies and think creatively	Ability to: • Research and apply critical-thinking techniques to analyse information, identify connections and develop evidence-based insights • Proactively identify and address issues and potential problems that may have a negative impact on departmental objectives, employees or end users • Generate creative new ideas and options to address issues and improve the customer or stakeholder experience • Seek contributions and ideas from people with diverse backgrounds and experiences • Collaborate to identify, share and implement business process improvements that address shared challenges, resolve issues and enhance operational effectiveness • Analyse data and information to generate meaningful insights, communicate findings clearly, and advocate for process improvements that enhance business effectiveness and support objectives	Proficient
Business Enablers	**Risk and Governance** Proactively manage risks, take responsibility of own actions and uphold policy and legislation	Ability to: • Ensure your own actions and those of your team remain focused on achieving departmental outcomes • Exercise delegations responsibly and in accordance with departmental requirements • Understand and apply high standards of financial probity in the use of public funds and other resources • Identify and implement safe work practices, using a systematic risk management approach to ensure health and safety of self and others • Identify risks that may impact the achievement of goals and take appropriate steps to mitigate, manage or document those risks	Proficient
	Technology Maximise efficiency and effectiveness using technology	Ability to: • Leverage a range of technologies to enhance collaboration and streamline workflows • Monitor and ensure adherence to cyber security protocols and technology usage policies • Identify and implement strategies to optimise the use of available technology to achieve business strategies and outcomes • Ensure compliance with departmental records, information, and knowledge management policies to maintain data integrity and accessibility	Proficient

People Management	**Lead and Develop People** Guide, empower and motivate employees in a way that develops their capabilities and expertise.	Ability to: • Work collaboratively with others to set clear performance expectation deadlines that align with established performance frameworks • Proactively identify opportunities to build team capability and support to realise their potential • Provide specific, timely and actionable feedback that reinforces streng supports improvement • Identify and act on opportunities to coach and mentor others to enhan individual and team development • Recognise emerging performance issues and take appropriate steps to and resolve them • Effectively support and manage team members working flexibly and in locations • Create a psychologically safe environment where people's diverse bac and perspectives are respected and valued • Actively seek feedback on own leadership approach and reflect on opp for continuous improvement •	Intermediate

Corporate responsibilities

Employees are responsible for:

- Maintaining a commitment to the Code of Ethics for the South Australian Public Sector, and the legislative requirements of the Public Sector Act 2009 (SA) and Work Health and Safety Act 2012 (SA)
- Keeping accurate and complete records of business activities in accordance with the State Records Act 1997 (SA)
- Creating and maintaining a diverse, accessible, inclusive and culturally safe workplace to enable us to reflect our community
- Acting in a manner that is non-threatening, courteous, respectful, and consistent with DPC's accreditation as a White Ribbon workplace at all times
- Demonstrating a genuine commitment to Reconciliation, and the achievement of Reconciliation Action Plan outcomes.