Government of South Australia
Department of Treasury and Finance

Role Statement

Role title	Cyber Security Advisor Risk and Assurance	**Classification**	ASO5
Branch	Office of the Chief Information Officer	**Type of Appointment**	Term
Section	Cyber Security Directorate	**Position Number**	P45365
Approved by	Deputy Director, Internal Operations & Governance	**Date**	November 2025

Department of Treasury and Finance

The Department of Treasury and Finance is the lead agency for economic, digital and financial policy outcomes.

We play a vital role in providing financial services to the community and economic and fiscal policy advice as well as digital services to the Government of South Australia.

The Department of Treasury and Finance actively promotes flexible working arrangements and values diversity in the workplace.

Our Purpose

We are *the Government's trusted fiscal, economic, digital and policy advisor*.
We work to ensure *South Australia is a thriving, prosperous State now and in the future*.

Who we are

Talented, Clear Eyed and Curious

We are analytical, evidence based, innovative and creative.

High Performing

We are known for achieving successful and timely outcomes.

Trusted Partner

We work better together. We lead, partner, and collaborate to help solve the big challenges.

Agile

We organise around opportunities critical to our state and are flexible in responding to challenges.

Fulfilled and Fun

We take the work seriously and ourselves less so - we support each other in the pursuit of excellence and make Treasury a great place to work.

What we are known for

A world class Treasury and Finance.
A high performing agency that *seizes opportunities*, addresses the *big challenges*,
and is a *destination employer* providing *rewarding careers*.

Branch/Section

The Office of the Chief Information Officer (OCIO) enables a more connected and secure government so that South Australian (SA) Government agencies can better serve our community. We do this by leading the SA Government's technology, cyber security, and digital government strategies, as well as developing and delivering resilient and innovative ICT, digital and cyber security services, platforms, and critical infrastructure to SA Government agencies that are accessible, trusted and secure.

As well as working within the SA Public Sector Code of Ethics, OCIO's principles are: customer-centric and collaborative, growth minded, engaged and skilled, and honesty in action.

OCIO supports flexible work arrangements, and our office environment is activity-based, with spaces tailored for focused work, collaboration, and general space for everyday work.

Cyber Security Directorate, in OCIO, sets the state's cyber security agenda and leads SA Government's cyber security efforts by proactively identifying threats, responding to incidents, promoting best practice, and working with SA Government agencies to assist in coordinating, evaluating, and improving cyber security capabilities across government to ensure the security of government's information and systems.

What this role is responsible for

The Cyber Security Advisor Risk and Assurance is responsible for the provision of specialist advice and expertise to stakeholders across the department and government agencies. The Cyber Security Advisor Risk and Assurance will support cyber security policy, assurance, risk advisory and third-party risk management functions within the Cyber Security Directorate including working with stakeholders across the SA Government cyber security community.

- Develop cyber security risk, assurance and advisory practices and initiatives aligning to the South Australian Cyber Security Framework (SACSF) and South Australian Protective Security Framework (SAPSF).
- Develop and manage the automated governance, risk and compliance, and third-party risk management processes and tools, taking into consideration requirements from a diverse range of stakeholders.
- Contribute to risk advisory functions including cyber security program advice, across government cyber risk management, and cyber security documentation development and review.
- Develop and deliver assurance processes to monitor the performance of cyber security policy and third-party risk management requirements across government.
- Provide expert cyber security advice on risk, cyber security management and third-party risk to South Australian Government agencies.
- Develop project briefs, business cases and project proposals for cyber security related projects.
- Contribute to key initiatives to uplift cyber security for the South Australian Government.
- Coordinate with other state and commonwealth government agencies on policy, risk and assurance activities.

Who this role reports to

- Manager, Cyber Security Risk and Assurance

Key Relationships/Stakeholders

- Manager, Cyber Security Risk and Assurance.
- Staff within Office of the Chief Information Officer and across Department of Treasury and Finance.
- A range of internal and external stakeholders on matters relating to cyber security policy, risk and assurance.
- The Procurement and Commercial Branch on matters relating to supplier cyber risk management.
- Counterparts across all states and territories.

Special Conditions

- Applicants will be required to undergo the appropriate and relevant employment screening assessment(s) required for this role in line with the department's Employment Screening Policy. This role requires:
  - ☒ National Police Check
  - ☒ Working with Children Check
  - ☒ Security Clearance (Negative Vetting Level 1)
- The incumbent will be required to participate in the Departmental Performance Management Program.
- The incumbent may be required to be assigned to other positions at the same remuneration level across the department.
- Some out of hours work may be required. Intrastate and interstate travel may be required.
- Work within a confidential, commercially orientated and at times politically sensitive environment.
- The State Emergency Management Plan details a requirement for a Control Agency for Cyber Crisis. OCIO personnel will participate in Control Agency responsibilities as required subject to appropriate training and induction.

Essential Expertise

- Tertiary qualifications in cyber security, information technology or other relevant field, and / or relevant security training and certifications.
- Knowledge of information security frameworks.
- Knowledge of information security management, risk management and assurance practices.
- Experience in communicating and developing reports and related documentation in a clear and concise manner.
- Demonstrated ability to develop new processes, analyse existing processes, and implement improvements.
- Demonstrated ability to plan and coordinate activities using initiative to achieve outcomes within tight timeframes.
- Demonstrated ability to communicate effectively, in writing and verbally, with a wide range of people from both technical and non-technical backgrounds.
- Demonstrated ability to analyse issues, propose solutions, provide advice and present recommendations to stakeholders, both verbally and in writing.
- Demonstrated ability to work independently as well as collaboratively in a team environment and to manage and prioritise demanding workloads to a high standard.
- Keen attention to detail with the ability to work independently and manage multiple tasks effectively.
- Demonstrated problem-solving and innovation skills and experience identifying risks and driving improvements.
- Demonstrated experience in the application of the relevant legislation, policies and procedures, including Code of Ethics, EEO and cultural inclusion.
- An understanding of the legislative requirements of the *Work Health and Safety Act 2012*.
- An understanding of and ability to work/manage to the spirit and principles of AS ISO 31000:2018 Risk management – Guidelines.

Desirable Expertise

- Knowledge of Government policies, process and procedures relating to risk and cyber security.
- Knowledge of the South Australian policy frameworks including the SA Cyber Security Framework (SACSF) and SA Protective Security Framework (SAPSF).