Government of South Australia
Department of Treasury and Finance

Role Statement

Role title	Cyber Security Officer	**Classification**	ASO4
Branch	Office of the Chief Information Officer	**Type of Appointment**	Term
Section	Cyber Security Directorate	**Position Number**	P45363
Approved by	Deputy Director, Internal Operations and Governance	**Date**	20 April 2026

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 Officer contributes to the provision of specialist cyber security advice and expertise to stakeholders across the department and to government agencies. The role will support the delivery of cyber security policy, assurance and risk advisory, and third-party risk management functions across government. The role will:

- Contribute to 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).
- Support the development and management of automated governance, risk and compliance, and third-party risk management processes and tools, taking into consideration requirements from a diverse range of stakeholders.
- Participate in the development and maintenance of a standardised toolkit that can be leveraged by agencies to support their cyber security program implementation.
- Support assurance processes to monitor the performance of cyber security policy and third-party risk management requirements across government.
- Provide cyber security advice on risk, cyber security management and third-party risk to South Australian Government agencies.
- Undertake minor cyber security 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

- The Cyber Security Officer reports to the Manager, Cyber Security Risk and Assurance.

Key Relationships/Stakeholders

The Cyber Security Officer works closely with:

- A range of internal and external stakeholders on matters relating to cyber security policy, risk and assurance.
- The Department of Treasury and Finance on matters relating to supplier cyber risk management.
- Counterparts in other jurisdictions including the Australian government and state and territory governments.

Special Conditions

- Applicants will be required to undergo the appropriate and relevant Employment Screening Assessment(s) required for this role. This role requires:
  - ☒ Nationally Coordinated Criminal History Check
  - ☒ Working with Children Check
  - ☒ Security Clearance (Negative Vetting Level 1)
- Some work outside normal hours and some Intrastate and interstate travel may be required.
- 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.
- 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

- Relevant experience in a similar role.
- Demonstrated knowledge of information security management, risk management and assurance practices.
- Proven ability to communicate clearly, concisely and effectively, both verbally and in writing.
- Ability to undertake research, analyse information and provide input into projects and briefs.
- High level of organisational skills, including ability to meet tight deadlines and manage conflicting priorities.
- Tertiary qualifications in cyber security or other relevant field, and / or relevant security training and certifications.
- 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.
- Demonstrated knowledge of the South Australian policy frameworks including the SA Cyber Security Framework (SACSF) and SA Protective Security Framework (SAPSF).

Professional/technical ICT capabilities (Skills Framework for the Information Age – SFIA)

Information security: Level 4 - Provides guidance on the application and operation of elementary physical, procedural and technical security controls. Explains the purpose of security controls and performs security risk and business impact analysis for medium complexity information systems. Identifies risks that arise from potential technical solution architectures. Designs alternate solutions or countermeasures and ensures they mitigate identified risks. Investigates suspected attacks and supports security incident management.

Specialist advice: Level 4 - Provides detailed and specific advice regarding the application of their specialism to the organisation's planning and operations. Actively maintains knowledge in one or more identifiable specialisms. Recognises and identifies the boundaries of their own specialist knowledge. Where appropriate, collaborates with other specialists to ensure advice given is appropriate to the organisation's needs.