Government of South Australia
Department of Treasury and Finance

Role Statement

Role title	Senior Cyber Security Specialist	**Classification**	ASO6
Branch	Information and Technology	**Type of Appointment**	Ongoing
Section	Information and Technology	**Position Number**	P34926
Approved by	Chief Information Officer	**Date**	March 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*.

Information & Technology Branch

The Information and Technology (I&T) branch plays an important role for the department responsible for a full suite of centrally delivered digital services, ranging from high quality support to the delivery of innovative and transformative initiatives, to assist in enabling our commitment to being a world class Treasury.

What this role is responsible for

- Manage and maintain the cyber security governance framework, including policies, standards, procedures and supporting systems.
- Lead cyber security governance and risk management activities, including maintaining risk/issue registers, documenting risk treatments and escalating in line with agreed governance.
- Support delivery of the Cyber Security Program by planning and coordinating work items, schedules, dependencies and status reporting, applying initiative and judgement to meet timeframes.
- Undertake or contribute to investigations into activities that breach security standards and policies, including preparing clear written advice and proactively communicating outcomes to relevant senior stakeholders.
- Lead or participate in security audits, compliance reviews and other assurance activities; report on outcomes and coordinate remedial actions to address findings.
- Contribute to the development and achievement of Cyber Security business plan objectives.
- Maintain effective working relationships to support the delivery of ICT projects, training and other tasks by consulting, negotiating and communicating effectively with internal and external stakeholders (technical and non-technical).
- Contribute to the promotion and implementation of Public Sector Principles and Practices, including Equal Opportunity and Work Health and Safety, by adhering to relevant Acts and associated legislation

Who this role reports to

- Assistant Director, Cyber Security

Key Relationships/Stakeholders

- Contributing to the design and implementation of a digital 'centre of excellence' for the department, a centre that those within the department value and want to work with based on the quality of service, advice and the outcomes it delivers.
- Operating in a highly complex, very large and rapidly changing technical environment and being responsive to national and international developments in technology.
- Working effectively in a complex and changing organisation that is subject to social and regulatory imperatives and obligations.
- Contributing to the building of a productive and ethical work culture that can readily adapt to rapid economic, social or political change.
- Contributing towards establishing DTF as a cyber security leader within the state's public service, utilising the right technology, the right way to enable the business.

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:
  - ☐ Nationally Coordinated Criminal History Check
  - ☐ Working with Children Check
  - ☒ Security Clearance (including Baseline, Negative Vetting Level 1 or Level 2, Positive Vetting)
  - ☐ Other:
- Some out of hours work may be required. 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.

Essential Expertise

- Demonstrated knowledge of current security controls and solutions, including the application of risk management techniques to design, deploy and operate security services that deliver practical business outcomes.
- Demonstrated ability to develop new processes, analyse existing processes, and implement improvements to cyber security controls, governance and assurance activities.
- Experience in systems audit and compliance review for cyber security, including tracking findings and coordinating remediation actions.
- Experience with control testing against recognised industry frameworks.
- Experience with vulnerability management practices, including prioritisation of remediation based on risk and business impact.
- Proven successful experience building strong/constructive relationships and networks, including the ability to consult, negotiate and influence with a range of stakeholders and customers across Government and industry at technical and managerial levels.
- Proven ability to plan and coordinate activities using initiative and judgement to achieve outcomes within tight timeframes, including managing dependencies and risks/issues.
- Proven ability to communicate effectively, in writing and verbally, tailoring messages for technical and non-technical audiences (including concise briefings and clear written advice).
- 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

- Certification in a relevant cyber security discipline (i.e. CISM, CISSP, CRISC, Security+ etc.)
- Azure security certification