



POSITION DESCRIPTION

Directorate: Digital Canberra

Position Number: P54512

Division: Customer, Data and Technology

Classification: Senior Officer Grade B

Business Unit: ACT Cyber Security Centre – Governance, Risk and Assurance Team

Location: Hybrid working arrangements (Winyu and work from home)

Position Title: Director, Cyber Security Governance and Policy

Last Reviewed: July 2026

AGSVA Baseline level = Position of Trust (PoT)

The successful applicant must be an Australian citizen and possess or acquire and maintain an Australian Government Security Vetting Agency (AGSVA) security clearance at the Baseline level as an eligibility qualification. If AGSVA screening is not successful, your employment will not commence or, if already commenced, your employment will be reassessed.

The Australian Capital Territory Public Service (ACTPS) is a values-based organisation where all employees are expected to embody the prescribed core values of respect, integrity, collaboration and innovation, as well as demonstrate the related [signature behaviours](#).

DIRECTORATE OVERVIEW

Digital Canberra (DCBR) leads the ACT Government's technology, digital, data, and cyber security services. We strive to improve the lives of Canberrans through delivering and supporting digital government services that are easy to access, save time, and are safe to use. We achieve this while also looking to the future – making technology investment decisions that will transform Canberra into a genuinely connected city.

Digital Canberra leads the implementation of the [ACT Digital Strategy](#) and [ACT Digital Health Strategy](#), manages ICT infrastructure for our hospitals, schools, and public service, and represents the ACT at national digital, data, and cyber security forums.

Digital Canberra has a diverse workforce across many functions and sites. We have an inclusive culture, and we ensure our people are respected, valued, and involved.

DIVISION OVERVIEW

The **Customer, Data and Technology Group** enables a modern, digitally empowered ACT Government. By delivering shared services that are efficient, secure, AI-enabled, and customer-focused the group helps ensure that citizens and businesses benefit from responsive, transparent, and innovative public administration.

The group has a wide range of strategy, policy and operational responsibilities across ACT Government including:

- management of Information Communications Technology services,

- service integration and management
- program and project management
- Cyber, risk and governance
- strategic asset management
- data and artificial intelligence (AI) including digital records.

BUSINESS UNIT OVERVIEW

ACT Cyber Security Centre

ACT Cyber Security Centre (ACTCSC) provides a secure and trustworthy ICT environment for services. ACTCSC offers first line of defence from cyber-attacks on government IT and data assets. We improve ACT Government's cyber security posture through innovation, collaboration, and education.

POSITION OVERVIEW

The Cyber Security Governance, Risk and Assurance (GRA) team sits within the ACT Cyber Security Centre and leads whole-of-government cyber security policy, governance, risk and assurance functions. The team is responsible for developing and maintaining cyber security policies, standards and governance frameworks, and for providing independent security risk assessment and assurance services across ACT Government ICT systems and infrastructure.

The Director role plays a pivotal function across the team to support development and review of security risk assessments, mentor team members in cyber security best practice and contribute to the development of cyber awareness material. You will also lead and contribute towards improvements to processes for delivering ICT security risk management and compliance across ACT Government. Additionally, the Director supports the creation and maintenance of cyber policies, standards, processes, plans, guidelines, and templates, with the support of technical cyber security staff.

The Director also contributes to the governance reporting requirements of the team by assisting with the creation of a broad range of governance and reporting artefacts including ministerial correspondence and briefs including cabinet submissions, business cases and other key documents.

The role requires excellent time management skills and attention to detail to develop, implement, and maintain processes and procedures to ensure that branch correspondence and reporting outputs are timely, accurate and comprehensive.

The current government and Executive support hybrid working for positions of this nature, noting this may be subject to change in future.

WHAT YOU WILL DO

Under the broad direction of Senior Director, Governance Risk and Assurance and the ACT Government Chief Information Security Officer (CISO) you will:

1. Support the development and implementation of cyber security governance including the whole of government cyber security framework, security policies, and compliance controls in collaboration with key stakeholders.
2. Provide strategic advice and briefings to DCBR, directorates and ministers on cyber security related matters.

3. Manage and implement cyber security initiatives including developing proposals and business cases.
4. Conduct and perform quality assurance of risk assessments and contribute to the development and improvement of processes for delivering ICT security risk management and compliance.
5. Generate and report on security metrics and performance for internal stakeholders, internal and external audit, and other stakeholders.
6. Represent the ACT Cyber Security Centre at meetings, committees, and seminars.
7. Assist with the development and implementation of cyber security awareness initiatives to lift cyber security awareness across the ACT Government.
8. Mentor and develop junior staff in the ACT Cyber Security Centre.
9. This position may involve direct supervision of staff.

WHAT YOU REQUIRE

The information below describes the capabilities that are required to perform the duties and responsibilities of the position.

Professional / Technical Skills and Knowledge

1. Formal education qualifications, professional certification or extensive experience in a related subject area, ICT Security, Risk Management, Auditing, Governance or Project Management will be highly regarded.
2. Demonstrated ability to identify cyber security vulnerabilities from system designs and vendor service information, analyse and measure risks, and recommend treatments as part of the development of security assessment reports to support ACT Government.
3. Demonstrated ability to deliver high-quality reports, ministerial briefings, and advice to senior executives and other stakeholders.
4. Demonstrated ability to plan and organise activities well in advance, prioritise own workloads and meet set deadlines and delivery expectations whilst considering changing circumstances.
5. Analytical thinking and problem-solving skills to resolve immediate problems for customers and proactively design solutions to achieve better security outcomes.

Behavioural Capabilities

1. Ability to liaise effectively with a variety of stakeholders internally, within the business and externally (vendors/external auditors).
2. Well-developed verbal and written communication skills with a high level of attention to detail, including the ability to accurately clarify, check, and present information.
3. Expert leadership in delivering agreed strategic business outcomes and solutions by taking initiative, encouraging transformational change and improved service delivery, supporting resources across different technical areas, setting clear direction, and providing guidance for internal DCBR teams.
4. Ability to plan and organise activities well in advance, prioritise workloads and meet set deadlines, considering changing circumstances.
5. Foster a positive culture and team that recognises and values diversity and uses knowledge of differences to develop best practice service to all stakeholders.
6. Upholds and models the ACTPS Values and Signature Behaviours, particularly in changing circumstances and while managing multiple priorities and demands.

Compliance Requirements

1. Australian citizen and possess, or acquire and maintain, an Australian Government Security Vetting Agency (AGSVA) security clearance at the Baseline level.
2. This position does not require a pre-employment medical.
3. This position does not require a Working with Vulnerable People Check.