



POSITION DESCRIPTION

Directorate: Digital Canberra

Position Number: P54411

Division: Customer, Data and Technology

Classification: Senior Officer Grade A

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

Location: Hybrid working arrangements (Winyu/ Work from home/ Onsite other locations as required)

Position Title: Senior Director, Cyber Security Governance, Risk and Assurance

Last Reviewed: July 2026

Position Requirements:

AGSVA Negative Vetting 1 (NV1) 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 Negative Vetting 1 (NV1) 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.

As the Senior Director, you will provide strategic leadership for the ACT Government's cyber security governance, policy, risk and assurance functions, setting the direction for a contemporary and risk-based approach to cyber security across government. You will lead a high-performing, multidisciplinary team and foster a culture of collaboration, innovation, accountability and continuous improvement to ensure the delivery of trusted, client-focused services and advice.

Working closely with directorates, DCBR teams, vendors, industry partners and senior executives, you will build strong relationships and influence decision-making on complex and emerging cyber security issues. You will drive the development and implementation of whole-of-government cyber security strategies, policies, governance frameworks and assurance programs that align with government priorities and evolving threat and regulatory environments.

The role is responsible for identifying opportunities to strengthen cyber security capability, maturity and resilience across government through strategic initiatives, service improvements and the adoption of better practice governance and risk management approaches. You will lead organisational change and cyber security uplift programs, promote a culture of informed risk management, and ensure governance frameworks remain effective, fit-for-purpose and responsive to emerging challenges.

As a senior leader, you will provide authoritative advice to executives, governance committees and stakeholders on cyber security risks, priorities and investment decisions. You will influence strategic outcomes across government, drive continuous improvement in cyber security services and practices, and champion initiatives that strengthen the ACT Government's overall cyber security posture, resilience and preparedness.

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 the ACT Government Chief Information Security Officer (CISO) you will:

1. Engage with internal Digital Canberra teams, business clients across the Territory directorates, solution vendors and external stakeholders on security related matters.
2. Provide ICT security advice including policy, administrative, technical, and professional advice to business customers.
3. Undertake research and analysis to perform security risk assessments and compliance audits of ICT systems and infrastructure to produce associated reports.
4. Develop, implement, and maintain ICT security risk and compliance frameworks, policies, processes, and plans.
5. Maintain and improve business processes for delivering high quality cyber security risk management services to business clients.
6. This position does 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 and/or extensive experience in a related subject area, Cyber Security Risk Management, ICT Security, Risk Management, Auditing, Governance or Project Management, will be highly regarded.
2. Experience in performing risk management assessment or developing System Security Plans will be highly regarded.
3. 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.
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. 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.
2. The ability to handle sensitive material with confidentiality, showing sound judgement and maturity.
3. Demonstrated ability to influence and negotiate with business and senior leadership.

Compliance Requirements

4. Australian citizen and possess, or acquire and maintain, an Australian Government Security Vetting Agency (AGSVA) security clearance at the Negative Vetting 1 (NV1).
5. This position does not require a pre-employment medical.
6. This position does not require a Working with Vulnerable People Check.