ARPC Position Description

Role Title:	Information Security Specialist		
Function:	Operations	**Classification broadband:**	ARPC 6
Location:	Sydney	**Security clearance:**	Baseline
Role Reports to (role title)**:**	Director of Information Security		
Direct Reports (role titles)**:**	Nil		

Purpose of the role (Why the role exists; how the role contributes to the ARPC's strategic objectives)

The Information Security Specialist provides information security advice, assessment and assurance across ARPC's business and technology environment. The role helps decision-makers understand security risks, evaluate control design and evidence, and make informed decisions.

Reporting to the Director of Information Security, the role works with business, technology, data, risk and supplier stakeholders. It supports information security governance and challenge without owning operational delivery, production changes or remediation.

Key Accountabilities (Key activities, tasks, and outcomes to be achieved)

The position is expected to perform the following activities:

- Conduct information security assessments for technology, cloud, data, supplier and business change initiatives.
- Provide practical security advice to project teams and business owners from planning through implementation and transition.
- Assess security risks, control design and supporting evidence, then document clear recommendations and required actions.
- Review proposed architectures, solution designs and changes to identify security requirements and control gaps early.
- Support Operations and governance activities including policies, standards, risk assessments, control assessments and security exceptions.
- Review remediation evidence and advise whether identified security issues are ready for governance closure.
- Support third-party security assessments and define security requirements for procurement and supplier reviews.
- Analyse vulnerabilities, incidents, control issues and assurance results to support management and committee reporting.
- Maintain clear assessment records, action tracking and evidence so security decisions can be reviewed and supported.
- Support incident governance, post-incident reviews and security exercises without owning containment, recovery or technical remediation.

Working Relationships (Key stakeholders, clients, customers, suppliers, providers, consultants, etc.)

Build and maintain strong relationships within:
Internal: Information Technology, Information Security, Actuarial, Claims, Underwriting, Finance, Risk, and broader ARPC teams.
External: Implementation partners and specialist consultants engaged by ARPC as required.

Person specification

Qualifications and experience

Qualifications

- Tertiary qualification in information technology, cyber security or related discipline - Desired.
- Relevant industry certification or training in information security, risk, audit or assurance - Desired.
- Commitment to maintain relevant professional development and security knowledge - Mandatory.

Experience (minimum type and level of experience required to perform the role)

- 5–8 years of relevant information security experience, including consulting, advisory, governance, risk or assurance work – Mandatory
- Experience leading security assessments and translating technical evidence into clear risks, recommendations and business decisions – Mandatory
- Experience assessing cloud, identity, endpoint, network, data protection, vulnerability, monitoring, software and service controls – Mandatory
- Experience applying the Australian Government Information Security Manual (ISM), Essential Eight or comparable security frameworks – Highly Desirable
- Experience conducting security risk assessments, control reviews and evidence-based assurance activities – Mandatory
- Experience reviewing supplier security, procurement requirements or third-party assurance evidence – Desired

Technical Capabilities (skills, knowledge, technical or specialist capabilities)

- Strong knowledge of information security governance, risk management, security controls and assurance practices
- Ability to assess technical security evidence and translate findings into clear risks, recommendations and practical business actions
- Ability to develop and maintain security policies, standards and supporting governance documentation
- Strong understanding of AI, cloud, identity, endpoint, network, data protection, vulnerability management, monitoring, software and service security controls
- Strong written and verbal communication skills, including preparation of concise assessment reports, governance papers and management reporting
- Strong stakeholder management skills across business, technology, data, risk and external service providers
- Ability to analyse security data and present trends through reporting or visualisation tools – Desired
- Scripting, automation or data analysis capability to support repeatable security assessment and reporting activities – Desired
- Adopt, leverage AI capabilities as part of ongoing work efficiency and automations.

Key legislative / regulatory role responsibilities

Public Interest Disclosure Act 2013 (PID Act)

- ARPC staff must assist the ARPC CEO (or delegate) and/ or the Commonwealth Ombudsman in the conduct of a PID investigation.

Privacy Act 1988

- ARPC staff must adhere to the Australian Privacy Principles and the ARPC Privacy Policy and report any privacy breaches by any employee or contractor to the Privacy Officer /or Privacy Champion as soon as they become aware of them.

Freedom of Information Act 1982 (FOI Act)

- ARPC staff are responsible for notifying and supporting the Information Public Scheme (IPS) Team to ensure published website Information is accurate, up-to-date and complete.
- ARPC 'owners' of website content are required to review content on their page(s) at least annually.

Work Health & Safety Act 2011 (WHS Act)

- All workers, including senior managers and executives, have duties under WHS Act.
- These duties include taking reasonable care for our own psychological and physical health and safety and that your actions or omissions do not adversely affect the health and safety of other persons.

Authorities	Limits/ Type
Financial Delegations:	As per ARPC Delegations Policy
HR Delegations:	As per ARPC Enterprise Agreement
Declared Terrorist Incident (DTI) and Declared Cyclone Event (DCE):	As per ARPC Event Response Policy

ARPC Values
Integrity Respect Service Wellbeing

ARPC Capabilities (Integrated Leadership System)
ARPC Capabilities describe behavioural expectations for all employees, by classification broadband.

- Shapes strategic thinking
- Achieves results.
- Supports/cultivates productive working relationships.
- Exemplifies personal drive and integrity.
- Communicates with influence

Approved by: *(Name & position)*	Victoria Simpson (Chief Operations Officer)	**Date:**	21 August 2026