



Cyber Security Lead

Leadership Position Detail

Reports To	Chief Information Security Officer or Deputy Chief Information Security Officer	Group	Technology Strategy, Assurance & Cyber
Leadership Classification	MRP2	Location	Canberra / Brisbane
Reports – Direct Total	4 - 8		

Organisational Environment

Airservices Australia is a government-owned organisation responsible for the safe and efficient management of 11 % of the world’s airspace and provision of aviation rescue fire fighting services at Australia’s busiest airports.

Our people are our greatest asset with a dynamic and diverse team operating from locations across the country – from bustling cities to regional and remote locations, including an island. This team keep Australia’s aviation industry safe every day of the year, both in the air and on the ground.

We connect people with their world safely – linking family and friends, generating economic activity, creating jobs, and facilitating trade and tourism.

Airservices is committed to fostering a culture that is diverse, inclusive, and respectful. We encourage motivated individuals who love what they do, value a service first mindset and embrace a challenge to explore a career with Airservices. In return you will be a valued team member, be offered flexibility and experience a meaningful career in an exciting, ever-evolving aviation industry.

Primary Purpose of Position

You will be responsible for leading one of several teams of highly skilled cyber security professionals. Each leadership role contributes to managing effective cyber security governance, operational risk, audit, compliance, and assurance. All these functions are integrated within the overall Chief Information Security Officer team, to deliver a collective outcome which strengthens the security posture of Airservices.

It will be your responsibility to apply strategic planning, leadership, and advisory skills to enhance our cyber security risk management, while supporting Airservices leadership in the development and execution of enterprise-wide security strategies.

Accountabilities and Responsibilities

Position Specific/s

- Cyber Security Operations Lead: Responsible for daily cyber security operations, and the lead for incident response coordination including the management of commercial delivery partners supporting operational security outcomes.
- Cyber Security Design and Assurance Lead: Responsible for managing the delivery of enterprise-wide security governance, including the secure by design process including the management of commercial delivery partners supporting cyber design and assurance outcomes.
- National Airways Cyber Security Lead: Responsible for supporting and enabling the design and implementation of fit for purpose cyber security aspects of aviation technology programs including the management of commercial delivery partners supporting programs of work.
- Enabling Technologies Cyber Security Lead: Responsible for supporting and enabling the design and implementation of fit for purpose cyber security aspects of enabling technology programs including the management of commercial delivery partners supporting programs of work.

People Leadership

- Appropriate and effective leadership of team
- Appropriate and effective engagement with key stakeholders

Compliance, Systems and Reporting

- Enterprise Risk management responsibilities
- Internal and external reporting obligations
- Internal and external compliance management and reporting

Safety

- Demonstrate safety leadership and behaviours consistent with enterprise strategies.
- Demonstrate safety behaviours consistent with enterprise strategies

Key Performance Indicators

Efficient, Effective and Accountable

- Management of the operational information security control environment
- Monitoring and report on the effectiveness of controls
- Identifying remediation and or risk management requirements and ensure they are managed to an agreed outcome.
- Negotiate treatments
- Responsible for compliance and assurance of supporting relevant formal framework obligations

Commercial

- Realisation of the capability benefits in accordance with contractual arrangements with suppliers and vendors

- Facilitate the uptake of capabilities provided as a service.
- Ensure continuous improvement of managed service providers through active management of the control environment.
- Provide advice to establish and maintain effective services contracts with partners.
- Management of Service Providers in accordance with contracts to ensure the delivery of benefits and outcomes
- Develop specifications, managing vendor evaluations including acquisition processes and participating in negotiations with suppliers to establish contracts for the provision of ICT products and services, ensuring suppliers are approved in accordance with Airservices procurement processes
- Ensure ongoing viability of ICT contracts through consultation with management and key stakeholders, cost analysis, and use of key performance indicators to monitor supplier performance and to ensure continuous improvements are identified through review and benchmarking processes
- Provide input into programs/projects to ensure ongoing compliance to Airservices security standards

Safety

- Compliance with safety, risk, environmental and any other standards
- Continue to deliver Airservices' record of Safety, Environmental, WHS, Risk and Compliance excellence.
- Demonstrate safety behaviours consistent with enterprise strategies
- Continue to deliver Airservices' record of Safety, Environmental, WHS, Risk and Compliance excellence.

Leadership

- Leadership and management abilities, including the ability to lead leaders mentor talent.
- Well-developed interpersonal, representation and communication skills – including a proven ability to develop, influence and maintain productive working relationships at all levels.
- Proven track record of positively impacting organisational integration, cultural change and workforce engagement.

Key Relationships

- Senior Leaders - Provide operational and strategic advice and support to internal stakeholders on cyber security resilience through effective use of existing capabilities, risk management, and future planning.
- Business function and process owners - maintain effective working relationship with business function and process owners to influence and ensure obligations, objectives and requirements are operationalised.
- Managed Services Providers – Works closely with service delivery partners to ensure effective delivery of the enterprise-wide cyber security capability

Skills, Competencies and Qualifications

Technical, industry and subject matter:

- Exceptional skills and experience in managing cyber security in a complex enterprise
- Comprehensive working understanding of Australian government security requirements (ISM, PSPF, etc)

- Understanding attack vectors and how to design, articulate and measure effectiveness of security controls in traditional ICT and operational technology (OT) environments
- Ability to translate complex technical security issues through a business lens
- Extensive experience in delivering IT Security Management principles and delivery within an ITIL-based operational framework
- Good written and verbal communication skills, including presentations and reporting
- Strong soft skills in Negotiation, Prioritisation and Time Management
- Understanding of security architecture and technologies with a focus on developing, evaluating, and critiquing designs and integration approaches:
- Be able to articulate complex technical designs into requirements

Risk Management:

- Extensive experience in managing cyber security using a risk-based approach
- Working Knowledge of Risk Management, and its application in an information security context.
- Review and contribute to security assessments considering business criticality, information sensitivity and security objectives.
- Understanding of:
 - NIST 800-39 Managing Information Security Risk, and
 - NIST 800-37 Risk Management Framework for Information Systems

Management, communication, personal and interpersonal:

- A proactive approach to customer issues and problem resolution
- Well-developed communication skills, both written and verbal
- Excellent ability to build and maintain effective working relationships and engage with key internal and external stakeholders at all levels.
- Strong analytical skills with attention to detail.
- Ability to set clear objectives and monitor performance
- Ability to manage a team, including setting performance and objectives, managing resources and prioritising tasks.

Qualifications

- Formal academic qualifications in an Information Communications Technology (ICT) discipline or Cyber Security are highly desirable.
- Industry recognised qualifications in at least two of the following or similar are highly desirable:
 - CISSP – Certified Information Systems Security Professional
 - CISM – Certified Information Security Manager
 - SEC488: Cloud Security Essentials
 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling
 - FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics
 - ICS410: ICS/SCADA Security Essentials
 - FOR578: Cyber Threat Intelligence
 - FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response
 - CRISC – Certified Risk and Information Systems Control
 - CGEIT – Certified in the Governance of Enterprise IT
 - CISSP – ISSAP, ISSEP, ISSMP

Security Clearance

An Australian Government Negative Vetting Level 1 Security Clearance (or higher) eligibility is mandatory for this role.

Leadership Performance Standards and Behaviours

Airservices Leadership Standard of **Know Me, Focus Me** and **Value Me** is a clear articulation of how we expect our leaders to lead our people supporting a culture of trust, care, and accountability.

The Airservices value chain operating model provides the basis for cultural reform of Airservices, driven by empowered and accountable leaders working together to deliver results.

This role has a strong people focus where leadership is demonstrated through embedding positive employee experiences and new ways of working across the following:

Lead inclusively

- Lead, coach, develop and retain a high performing team by demonstrating authenticity and engaging our people with a Know Me, Focus Me and Value Me focus
- Every leader in Airservices must demonstrate constructive behaviours aligned with our values and target culture of trust care and accountability.

Think strategically

- Promote, support and guide teams to drive quality delivery whilst shifting mindsets to focus on continuous improvement and transformation.

Collaborate effectively

- Create and support an environment, which fosters an emphasis on collaboration and accountability to promote a trust-based, inclusive culture centred on principles of care and purpose.
- Develop and maintain a broad range of relationships to influence within the value chain at an Executive, peer and team level and positively influence internal key stakeholders.

Communicate with impact

- Create and support an environment, which fosters an emphasis on collaboration and accountability to promote a trust-based, inclusive culture centred on principles of care and purpose.

Deliver outcomes

- Lead our people effectively to collectively contribute and deliver on Airservices goals by optimising and developing business systems.

As a member of Airservices, you will consistently demonstrate performance standards and behaviours that meet our **Code of Conduct**. This includes:

- Treating everyone with dignity, respect, and courtesy
- Acting with honesty and integrity
- Acting ethically and with care and diligence
- Complying with all Airservices' policies and procedures, and applicable Australian laws
- Disclosing and taking reasonable steps to avoid any actual, potential, or perceived conflict of interest
- Behaving in a way that upholds our vision, mission, and values, and promotes the good reputation of Airservices.