Senior Engineer, Cybersecurity (fixed term)

This position description is designed to give an overview of the type of work and performance required for this role and may include other duties as required.

Who We Are

The Civil Aviation Authority of New Zealand is the country's aviation safety and security regulator. We are a Public Service Crown entity responsible through our Board to the Ministry for Cities, Environment and Transport (MCERT).. We regulate a wide range of aviation activities, from commercial airlines to private pilots, ensuring that all aspects of the industry meet the highest standards of safety and security. Our important work not only saves lives but also facilitates travel, recreation, commerce, and protects the environment. By ensuring a safe and secure aviation system, we provide confidence and safeguard the reputation of New Zealand, benefiting our country as a whole.

Our Vision and Purpose

Everything we do is related towards the achievement of 'a safe and secure aviation system – so people are safe and feel safe when they fly'.

Our Pathways

We have three pathways that lead us to delivering our vision and purpose:

1. **Leadership and Influence**
   Through regulatory leadership we influence a safe and secure civil aviation system for New Zealand.
2. **Active Regulatory Stewardship**
   We monitor and care for the civil aviation regulatory system through our policy and operational responsibilities.
3. **Professional Regulatory Practice**
   We act to identify risk and reduce it through intelligence-led intervention.

Our Values

Our organisation's Values support how we work to keep New Zealand skies safe and secure.

Collaboration - *Me mahi tahi*
We work together to achieve and succeed

Transparency - *Me mahi pono*
We are open and honest communicators

Integrity - *Me mahi tika*
We do the right thing

Respect - *Me manaaki*
We treat all people with consideration and kindness

Professionalism - *Kia tu rangatira ai*
We act in a way that brings credit to ourselves and our organisation

These feathers symbolise our Values, which are inspired by the sacred huia bird – a revered symbol of friendship, respect, leadership and mana.

Each feather in the Values has a different hue to reflect different aspects of the diversity, leadership, talent and experience our people bring to their work every day.

Our Values are us – we are many cultures, languages, genders, unique personalities and perspectives working together to achieve our Vision and Purpose.

Role Purpose

The Senior Engineer, Cybersecurity (fixed-term) leads the technical implementation of information security and cybersecurity related solutions, working across multiple initiatives and delivery workstreams to ensure security practices are adopted and delivered. Using expertise in security practices and tooling, the role identifies opportunities to improve CAA's digital infrastructure and security. The role translates security policies, standards, threat and vulnerability information and architecture principles into practical technical solutions that improve confidentiality, integrity, and availability outcomes. This is a subject matter expert role expected to advise the transformation programme and provide knowledge transfer into the Digital Engineering and Systems Administration team.

Key Dimensions

Group:	Digital Transformation and Technology	
Team:	Digital Engineering	
Reports to:	Team Leader, Digital Engineering	
Location:	National Office	
Salary Band:	18	
Financial:	None	Delegation Level = None
People:	Direct Reports = N/A	Delegation Level = None
Key Relationships:	Internal: • Digital teams • Principal Advisor, Cybersecurity • Business transformation programme team • Business and System owners	External: • Vendors and service providers
Essential requirement/s:	N/A	

Shared Accountabilities

- We work professionally, aligned with our Values, Code of Conduct and guiding CAA policies.
- We foster a safe, inclusive culture by respecting and embracing the diverse perspectives, experiences, and backgrounds of all.
- We ensure our work is aligned to our strategy, vision and purpose in our approach to delivering intelligence led, risk-based safety and security outcomes.
- We carry out work and conduct our relationships in a way that supports the CAA's commitment to the Te Tiriti o Waitangi.

- We work together to create an environment that keeps ourselves and others safe by following the responsibilities laid out in our people policies and our Health, Safety and Wellbeing Commitment statement.

Key Accountabilities

Deliver Technical Outcomes for Business Transformation - Lead the implementation of digital infrastructure, cyber security controls, and technology components required to deliver business transformation initiatives, ensuring solutions are secure, scalable, compliant, and operationally sustainable. Work with project and delivery teams to embed security requirements into solution design, procurement, implementation and operational processes.

Provide Technical Leadership and Expertise - Lead technical delivery activities, working closely with Business Transformation teams, architects, vendors, and Digital teams to deliver agreed outcomes and resolve complex technical challenges. Provide cyber security subject matter expertise, advice and guidance to business stakeholders, project teams and technology teams, translating security policies, standards, architecture principles and threat information into practical technical solutions.

Maintain Operational Stability and Performance - Monitor, optimise and support infrastructure, systems, networks and technology services to ensure availability, performance, security and reliability throughout project delivery and transition. Monitor cyber security events, threats and vulnerabilities, in conjunction with the Principal Advisor, Cybersecurity, supporting assessment, remediation, reporting and continuous improvement activities.

Improve and Automate Technology Services - Identify opportunities to streamline, automate and improve security controls, technology operations and service delivery, reducing manual effort while enhancing resilience, compliance and service quality. Support the identification, assessment and management of cyber security and technology risks and contribute to maintaining relevant risk registers.

Enable Successful Transition to Operations - Ensure transformation deliverables are effectively transitioned into business-as-usual operations through documentation, knowledge transfer, operational readiness, support planning, and the implementation of sustainable security practices, processes and controls.

Support Team Capability and Collaboration - Share knowledge, provide guidance to less experienced team members, and build strong working relationships across the organisation to support successful transformation outcomes. Promote cyber security awareness and knowledge transfer, in conjunction with the Principal Advisor, Cybersecurity, to strengthen organisational capability and support the ongoing uplift of Digital Engineering security practices.

Manage Technical Risks and Issues - Identify, assess and resolve technical security risks, incidents and operational issues, ensuring solutions align with long-term organisational and operational requirements. Support incident response activities, assurance reviews, audits, certifications and compliance assessments, and contribute to the continuous improvement of cyber security controls, processes and organisational resilience.

Competencies

Get Smart – Knowledge & Context: Level 2 ▪▪▫
Understands the role of the CAA within the aviation sector, and has a holistic understanding of the regulatory environment, the structure and interrelated operating practices of the CAA. Follows the guidance and processes expected of all CAA employees as a modern, adaptive regulator, set out in policies, legislation, aviation rules, and other internal documents.

Think Smart – Sound Judgement: Level 2 ▪▪▫
Makes appropriate and transparent decisions by analysing relevant information, takes into consideration different points of view, demonstrating the ability to make difficult and/or sensitive decisions. Has flexibility to both adopt a course of action and change it when required by the situation.

Work Smart – Achieves Results: Level 2 ▪▪▫
Drives change and results through effective planning, collaboration, and communication. Builds trust, fosters teamwork, and demonstrates self-awareness to achieve shared goals and continuous improvement.

Act Smart – Personal Effectiveness: Level 2 ▪▪▫
Is adaptable and resilient to meet changing needs and expectations. Displays self-awareness and is respectful of diversity. Takes responsibility for self-learning and development. Demonstrates behaviours consistent with the Code of Conduct and CAA Values.

Skills and Experience

- Microsoft Certified Expert certification (Essential)
- Experience with or knowledge in the following is advantageous:
  - Intel Based Architecture and Microsoft Systems and Applications.
  - Applying architecture documentation requirements into detailed design and implementation documents and articulating actions required.
  - Windows-based server configuration and maintenance. Virtual machine technologies, preferably including experience of VMWare ESX server.
  - Cybersecurity experience or qualification, such as CISSP, CEH, GIAC or equivalent
  - Experience and knowledge of secure cybersecurity architecture, offensive security, threat detection, protocols, digital forensics, secure coding and practices
  - Data storage (SAN and NAS) and back-up technologies and policies.
  - Problem identification and resolution.
  - Design documentation.
  - Incident Management. Software development (e.g. PowerShell automation, JavaScript, Pearl-Script).
  - Change Management.
  - Azure Cloud Services including AAD, Intune, ExO, M365, Landing Zone, Terraform.

Relevant Competencies under SFIA9

Infrastructure Operations (ITOP) Level 5

Provisioning, deploying, configuring, operating and optimising technology infrastructure across physical, virtual and cloud-based environments.

- Provides technical leadership to optimise the performance of the technology infrastructure.
- Drives the adoption of tools and automated processes for effective operational management and delivery.
- Oversees the planning, installation, maintenance and acceptance of new and updated infrastructure components and infrastructure-based services.
- Aligns to service expectations, security requirements and other quality standards.
- Ensures operational procedures and documentation are current and effective, tracks and addresses operational issues and reports to stakeholders.

Infrastructure Design (IFDN) Level 5

Designing technology infrastructure to meet business requirements, ensuring scalability, reliability, security and alignment with strategic objectives.

- Manages the design of infrastructure from analysis to execution and evaluation.
- Accountable for achieving design objectives and ensuring alignment with organisational goals and the effective integration of infrastructure components and systems.
- Provides authoritative guidance on design practices and methodologies.
- Evaluates new technologies and their applicability to the organisation's needs.
- Develops and enforces design standards and recommended practices, ensuring consistent and high-quality design outcomes.

Information Assurance (INAS) Level 5

Protecting against and managing risks related to the use, storage and transmission of data and information systems.

- Interprets information assurance and security policies and applies these to manage risks.
- Provides advice and guidance to ensure adoption of and adherence to information assurance architectures, strategies, policies, standards and guidelines.
- Plans, organises and conducts information assurance and accreditation of complex domains areas, cross-functional areas and across the supply chain.
- Contributes to the development of policies, standards and guidelines.

Systems Installation and Removal (HSIN) Level 5

Installing and testing, or decommissioning and removing, systems or system components.

- Takes responsibility for installation and/or decommissioning projects.
- Provides effective team leadership, including information flow to and from the customer during project work.
- Develops and implements quality plans and method statements.
- Monitors the effectiveness of installations and ensures appropriate recommendations for change are made.

Information Security (SCTY) Level 4

Defining and operating a framework of security controls and security management strategies.

- Provides guidance on the application and operation of elementary physical, procedural and technical security controls.
- Explains the purpose of security controls and performs security risk and business impact analysis for medium complexity information systems.
- Identifies risks that arise from potential technical solution architectures.
- Designs alternate solutions or countermeasures and ensures they manage identified risks.
- Investigates suspected attacks and supports security incident management.

Systems Design (DESN) Level 4

Designing systems to meet specified requirements and agreed systems architectures.

- Designs system components using appropriate modelling techniques following agreed architectures, design standards, patterns and methodology.

- Identifies and evaluates alternative design options and trade-offs.
- Creates multiple design views to address the concerns of the different stakeholders and to handle functional and non-functional requirements.
- Models, simulates or prototypes the behaviour of proposed system components to enable approval by stakeholders.
- Produces detailed design specifications to form the basis for the construction of systems.
- Reviews, verifies and improves own designs against specifications.

Emerging Technology Monitoring (EMRG) Level 4

Identifying and assessing new and emerging technologies, products, services, methods and techniques.

- Supports monitoring of the external environment and assessment of emerging technologies.
- Contributes to the creation of reports, technology road mapping and the sharing of knowledge and insights.