System and Security Specialist (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 Minister of Transport. 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 Systems and Security Specialist (fixed term) applies specialist knowledge to provide information and technology support that enables business transformation, regulatory effectiveness and supports operational performance of the CAA, with a focus on identity and access management, cybersecurity, software licensing, and internal systems.

Working across multiple initiatives and delivery workstreams this role empowers the usability, reliability, and security of the IT environment by enabling the secure and efficient operation of infrastructure and applications.

The Systems and Security Specialist contributes to security assessments, monitors compliance through assurance activities, implements mitigations, and coordinates responses to incidents, risks and issues, ensuring alignment with regulatory requirements and industry best practices. Through specialist input and expert guidance into IT operations, enterprise risk management, and digital enablement, the role supports informed decision making, and the development and enforcement of policies and procedures that align system provisioning and maintenance with business transformation objectives.

Key Dimensions

Group:	Digital Transformation and Technology	
Team:	Digital Engineering	
Reports to:	Team Leader, Digital Engineering	
Location:	Datacom Centre	
Salary Band:	16	
Financial:	Nil	Delegation Level = Nil
People:	Direct Reports = Nil	Delegation Level = Nil
Key Relationships:	Internal: • Principal Advisor, Cybersecurity • Wider Digital teams	External: • External cybersecurity vendors/licensing providers

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 CAA's commitment to Te Tiriti o Waitangi.

- We work together to create an environment that keeps ourselves and others safe and by following the responsibilities laid out in our Health, Safety and Wellbeing Commitment Statement which outlines the expectations of leaders and all staff.

Key Accountabilities

- Proactively triage and resolve cybersecurity threats by leveraging enterprise endpoint protection platforms, collaborating with peers and external vendors to investigate incidents and drive continuous improvements.
- Consistently enhance organisational security posture while advising leadership on emerging threats and advanced mitigation strategies that support business transformation projects and initiatives.
- Partner with vendors to lead vulnerability assessments, advanced scanning, and incident response initiatives aligned to programme and organisational outcomes.
- Investigate and respond to security breaches, escalating incidents with potential high impact, while also monitoring and actioning requests received through the cybersecurity channels to ensure timely and effective threat management. Provide support to the BAU teams if needed.
- Audit and update access control lists and security configurations for highly exposed groups and individuals, applying additional safeguards where required that support long-term transformation goals.
- Oversee enterprise software asset management and ensure licensing compliance across the organisation.
- Facilitate the full software licensing lifecycle, including working with vendors for pricing and terms, managing renewals, audits, and entitlements, and securing approvals for purchases and cost efficiency.
- Conduct comprehensive audits and analyses of software usage across the environment, collaborating with Digital teams to identify and remediate unauthorised applications. Conduct targeted software risk assessments and contribute to peer review processes to uphold organisational security and quality standards.
- Collaborate on digital strategy, enterprise risk management, and digital transformation initiatives.
- Actively engage across digital and business initiatives, providing advanced technical advice on cybersecurity, identity management, and system access. Audit data inputs and permission assignments created by other teams to ensure accuracy and compliance, while offering subject matter expertise to support secure and effective outcomes across the organisation.
- Serve as a key point of contact for system-related support requests, managing inquiries related to access, configuration, permissions, identity security, directory services, collaboration platforms, shared mailboxes, and distribution lists to ensure secure and efficient system operations.
- Administer internal business applications, overseeing user access provisioning and ensuring appropriate permission levels across enterprise platforms and approved applications.

- Maintain account records and administer access rights, including conducting regular audit reviews to ensure compliance and accuracy.
- When requested by senior leadership or oversight teams, handle confidential information through advanced search and reporting tools.
- Apply security controls and contribute to policy and procedure reviews, ensuring alignment with best practices and regulatory requirements.

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 analyzing 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

Essential

- Diploma in Information Technology Systems, Computer Science, or demonstrable equivalent experience in a related field.
- Minimum 5 years' experience in a support desk or equivalent technical role.
- Understanding of licensing models (Microsoft, Adobe, SaaS) and compliance frameworks.
- Experience with cloud platforms (Azure, AWS), virtualization, and automation (PowerShell, Python).
- Experience in cybersecurity practices, with working knowledge of Microsoft Defender and Purview for monitoring, investigation, and safeguarding organisational data.

- Experienced with Azure Cloud Services, including Azure Active Directory (AAD), Intune, Exchange Online (ExO), and Microsoft 365, supporting identity management, device compliance, and cloud-based collaboration tools.

Desirable Certifications include

CISSP, CISM, CISA, Microsoft Certified: Azure Administrator, and CompTIA Security+, or equivalent credentials demonstrating expertise in cybersecurity, cloud administration, and IT governance.

Relevant Competencies under SFIA9

Information Security (SCTY) Level 3

- Applies and maintains specific security controls as required by organisational policy and
- local risk assessments.
- Communicates security risks and issues to business managers and others.
- Performs basic risk assessments for small information systems.
- Contributes to the identification of risks that arise from potential technical solution
- architectures.
- Suggests alternate solutions or countermeasures to mitigate risks.
- Defines secure systems configurations in compliance with intended architectures.
- Supports investigation of suspected attacks and security breaches.

Application Support (ASUP)

- Follows agreed procedures to identify and resolve issues with applications.
- Uses application management software and tools to collect agreed performance statistics.
- Carries out agreed applications maintenance tasks.

Incident Management (USUP) Level 3

- Prioritises and diagnoses incidents applying agreed procedures and tools.
- Investigates causes of incidents and seeks resolution.
- Escalates unresolved incidents to higher levels or specialist teams.
- Coordinates with stakeholders to ensure timely resolution.
- Facilitates recovery, following resolution of incidents.
- Documents, communicates outcomes and closes resolved incidents.

Problem Management (PBMG) Level 3

- Investigates problems in systems, processes and services.
- Contributes to the implementation of agreed remedies and preventative measures.

Asset Management (ASMG) Level 3

- Applies tools, techniques and processes to create and maintain an accurate asset register.
- Produces reports and analysis to support asset management activities and aid decision making.
-

Identity and access management (IAMT) Level 3

- Administers standard identity and access management services, implementing policies
- and resolving related issues.
- Manages monitoring, audits and logging for identity and access management systems.
- Investigates minor security breaches in accordance with established procedures related to
- identity and access management.

- Assists users in defining their access rights and privileges.
- Designs and implements simple identity and access management solutions, enhancing
- user access security.
- Contributes to the enhancement and optimisation of existing identity and access
- management processes and systems.

Security Operations (SCAD) Level 3

- Investigates minor security breaches using established procedures, incorporating
- analytical tools and techniques.
- Performs non-standard operational security tasks adapting to evolving technologies and
- threat landscapes.
- Addresses and resolves a variety of security events to maintain system integrity and
- operational continuity.

Vulnerability Assessment (VUAS) Level 3

- Follows standard approaches to perform basic vulnerability assessments for small
- information systems.
- Supports creation of catalogues of information and technology assets for vulnerability
- assessment.