

Cloud Platform Engineer

Reports to:	Platforms and Infrastructure Manager	Position Status:	Permanent
Unit:	Digital and Technology	Location:	Avalon
Department:	Digital, Systems and Information	Team:	Platforms and Infrastructure
Direct Reports:	Nil	Budget & Delegated Authority:	Refer to Delegated Financial Authority Policy
Career Step:	7	Job Family:	Operations, Data & Technology
Career Path:	Specialist	Date:	September 2026

Role Purpose

The Cloud Platform Engineer is a technical specialist responsible for designing, engineering, automating, integrating and improving secure, resilient and cost-effective cloud and hybrid platform capabilities across Microsoft Azure, Amazon Web Services and relevant on-premises environments.

The role supports the evolution of Earth Sciences New Zealand's cloud operations and platform engineering capability by developing reusable standards, reference patterns, guardrails, automation and operating practices that help teams deliver reliable services at scale. Working across platform, application, science, cyber security, architecture, finance and vendor teams, the role provides practical cloud engineering advice, design assurance and hands-on support from early design through deployment, operational readiness and service transition. It helps ensure cloud and platform services are secure, observable, supportable, well governed and financially transparent, while reducing operational toil through infrastructure as code, DevSecOps practices, documentation and continual improvement. The role also contributes to incident response, problem resolution, knowledge sharing and capability uplift so that science, product and service teams can operate workloads safely, consistently and with confidence.

Position Priorities and Responsibilities

Cloud platform engineering, standards and operations

- Design, build and improve Azure and AWS landing zones, shared services and on-premises platform capabilities in line with agreed architecture, security and operational standards.
- Engineer and operate shared cloud capabilities across identity, networking, policy, secrets management, observability, backup, recovery, resilience and service integration.
- Support workload onboarding and migration from discovery and design through deployment, validation, operational readiness and service transition.
- Develop and maintain cloud platform standards, reference architectures, reusable patterns, guardrails and operating procedures.
- Provide technical advice, design assurance and risk-based recommendations for complex cloud and automation initiatives.
- Coach less-experienced engineers through pairing, peer review, knowledge sharing and clear documentation.

DevSecOps, automation and infrastructure as code

- Develop reusable Terraform, Ansible and configuration automation, using GitHub or GitLab workflows for peer review, testing, approvals and controlled deployment.
- Replace manual or error-prone activities with secure, repeatable automation that embeds security, privacy, resilience, cost and operational requirements.
- Integrate cloud services with identity, networking, security monitoring, service management, observability, financial management and on-premises platforms.
- Write automated tests, policy checks, configuration validation and documentation that confirm platform and service behaviour.

Cloud financial management and FinOps

- Contribute cloud engineering expertise to FinOps practices, including cost visibility, allocation, tagging, budgets and alerts, forecasting, consumption reporting, rightsizing and optimisation.
- Work closely with the Operations / Asset Analyst, Finance, project stakeholders and internal and external FinOps specialists.
- Provide technical data, automation and platform controls that support informed cost decisions while maintaining clear separation from budget ownership and financial approval responsibilities.
- Identify and recommend opportunities to improve cloud value and reduce avoidable expenditure without compromising agreed security, resilience or service outcomes.

Stakeholder enablement and delivery

- Build effective working relationships with DS&I platform, application and development teams, GeoNet, NSHM and other science projects and programmes to understand outcomes, constraints and support needs.
- Lead or contribute to cross-functional delivery teams, providing cloud engineering expertise from design through implementation and operational handover.
- Provide practical guidance, reusable examples and hands-on support that enable teams to adopt cloud, DevSecOps and platform engineering practices effectively.
- Communicate technical options, risks, dependencies and recommendations clearly to technical and non-technical stakeholders.
- Coordinate effectively with architects, cyber security specialists, vendors and service providers.

Operational excellence, documentation and capability uplift

- Maintain accurate architecture, configuration, operating, troubleshooting and support documentation for cloud platforms and automation.
- Ensure new and changed services meet operational-readiness requirements for monitoring, alerting, support, backup, recovery, documentation and ownership before production release.
- Monitor and support cloud and hybrid environments, diagnose complex performance, availability, capacity, configuration and integration issues, and implement durable remediation.
- Perform structured problem diagnosis and root-cause analysis, and lead improvements that reduce repeat incidents and operational toil.
- Plan and implement platform lifecycle activities, including upgrades, maintenance, patching, service improvements and decommissioning, using approved change and release practices.

- Participate in either the IT Operations or Cyber Security on-call roster, including associated incident response, problem management and service recovery activities.
- Maintain current knowledge of cloud, automation, container, virtualisation and DevSecOps practices and recommend improvements where they provide clear organisational value.

Responsibilities of all Employees

- Comply with all Earth Sciences New Zealand policies, procedures and frameworks, and act in line with the organisational values.
- Contribute to our healthy and safe workplace by following HSW expectations outlined in and integrated into our operational practises and HSW frameworks, including undertaking HSW training and participating in health-monitoring programmes relevant to your work.
- Work effectively as a team member by fostering good relationships and supporting others, providing coverage of other functions as required and ensuring workloads are evenly spread.
- Have the flexibility to adapt and develop as the organisation and its environment evolves.
- All employees are expected to uphold and demonstrate Earth Sciences New Zealand's values in their daily work. Our values guide how we work together, make decisions, and deliver outcomes, and are reflected through behaviours that contribute to a positive and inclusive workplace.

People Matter– Great work starts with how we treat each other

Stronger Together– We're at our best when we deliver together

Trusted Science– Trust is earned through the excellence of our work

Big Impacts– Our expertise makes a real difference for Aotearoa and beyond

Key Working Relationships

Internal	External
• Platforms and Infrastructure team • DS&I platform, application and development teams • Operations / Asset Analyst and Finance • Cyber Security, Architecture, Service Desk and Information Management • GeoNet and NSHM teams	• Platforms and Infrastructure team • DS&I platform, application and development teams • Operations / Asset Analyst and Finance • Cyber Security, Architecture, Service Desk and Information Management • GeoNet and NSHM teams

Person Specification

Qualifications and Experience

Essential

- A relevant tertiary or technical qualification, or equivalent demonstrated industry experience.
- Proven and sustained technical experience engineering and supporting production cloud infrastructure, with strong practical capability in at least one of Azure or AWS and the ability to work effectively across both.
- Demonstrated experience leading complex technical work and developing standards, reference patterns, guidelines or operating procedures.

- Practical experience with infrastructure as code and configuration automation, including Terraform and Ansible or closely related tools.
- Experience with Git-based engineering workflows using GitHub, GitLab or equivalent, including peer review, automated testing and deployment pipelines.
- Experience supporting cloud networking, identity and access, logging, monitoring, backup, security, resilience and cost-management capabilities.
- Experience diagnosing complex technical problems, assessing risk and implementing robust, documented and supportable solutions.
- Proven ability to collaborate across technical and stakeholder groups, provide expert advice, and coach or mentor other practitioners.

Desirable

- Relevant Azure, AWS, Terraform, Linux, security or DevOps certification.
- Experience with Azure services and patterns such as Azure Landing Zones, Management Groups, Azure Policy, Entra ID, Azure RBAC, Virtual Networks, Azure Firewall, Private Link, Application Gateway, Key Vault, Azure Monitor, Log Analytics, Azure Backup, Azure Site Recovery and Azure Kubernetes Service.
- Experience with AWS multi-account environments, AWS Organizations, Control Tower, IAM Identity Center, Service Control Policies, VPC networking, Transit Gateway, Route 53, CloudTrail, CloudWatch, Config, GuardDuty, Security Hub, Systems Manager, AWS Backup and container services.
- Experience with containers, Kubernetes, serverless services, APIs, event-driven integration or data-platform services.
- Experience supporting scientific, research, geospatial, high-performance computing or data-intensive workloads.
- Experience with scripting or software development using Python, PowerShell, Bash or a comparable language.
- Experience with IT service management, Agile delivery and production support practices.

Skills, Knowledge and Attributes

- Strong understanding of cloud architecture, infrastructure as code, automation, CI/CD and DevSecOps practices.
- Sound knowledge of cloud networking, identity, security, observability, resilience and cost-optimisation principles.
- Ability to write clear, maintainable code, tests and technical documentation and to review the work of peers constructively.
- Excellent analytical, diagnostic and problem-solving skills, with strong attention to detail.
- Ability to translate stakeholder outcomes into practical technical designs and communicate clearly with technical and non-technical audiences.
- A collaborative and service-oriented approach, with the confidence to respectfully challenge the status quo and improve established practices.
- Ability to plan and prioritise work across operational support and project delivery while maintaining appropriate governance and quality.
- Curiosity, initiative and an enduring commitment to learning, knowledge sharing and continuous improvement.

- Commitment to inclusive, culturally responsive ways of working, responsible stewardship, integrity and trust.