

GCP IAM Specialist - Cloud-Native Development

Job Information

Recruiter
NEXUS Corporation

Job ID
1607652

Industry
IT Consulting

Job Type
Permanent Full-time

Location
Tokyo - 23 Wards

Salary
Negotiable, based on experience

Refreshed
October 26th, 2026 00:00

General Requirements

Minimum Experience Level
Over 6 years

Career Level
Mid Career

Minimum English Level
Business Level

Minimum Japanese Level
Business Level

Minimum Education Level
Bachelor's Degree

Visa Status
Permission to work in Japan required

Job Description

We are seeking a highly skilled GCP IAM Specialist with strong cloud-native development expertise to design, implement, and govern identity and access management frameworks across our Google Cloud Platform estate. This role is pivotal in ensuring secure, compliant, and scalable access controls while driving cloud-native application delivery.

Job Description - Grade Specific

Key Responsibilities:

- Design and enforce IAM policies, roles, and permission boundaries across GCP projects, folders, and organizations
- Develop and maintain custom IAM roles aligned to least-privilege principles across multi-project GCP environments
- Build and maintain cloud-native applications and automation tooling using GCP-native services (Cloud Run, Cloud Functions, Pub/Sub, GCS)
- Implement Workload Identity Federation and service account management best practices
- Integrate IAM controls with CI/CD pipelines and enforce policy-as-code using Terraform
- Conduct IAM access reviews, audit log analysis via Cloud Audit Logs and Security Command Center
- Collaborate with development and platform teams to embed security controls into cloud-native delivery
- Define and maintain organization-level IAM guardrails using VPC Service Controls and Access Context Manager
- Drive IAM automation using Ansible playbooks for configuration management and drift detection

- Provide technical guidance and IAM governance frameworks to delivery teams

Required Skills

Required Qualifications

- 5+ years of hands-on experience with GCP IAM, including custom roles and policy management
- Strong proficiency in GCP-native development (Cloud Run, Cloud Functions, App Engine, Pub/Sub)
- Solid Terraform experience for IAM policy provisioning and infrastructure-as-code
- Experience with Workload Identity, service accounts, and federated identity management
- Proficiency in Python or Go for automation and tooling development
- Familiarity with GCP Security Command Center, Cloud Audit Logs, and compliance frameworks
- Experience implementing VPC Service Controls and organization policies
- Understanding of OAuth 2.0, OIDC, and SAML integration patterns on GCP

Preferred Qualifications

- Google Professional Cloud Security Engineer certification
- Experience with Ansible for IAM configuration drift detection
- Background in financial services, healthcare, or other regulated industries
- Familiarity with GKE Workload Identity and namespace-scoped IAM bindings
- Experience with SIEM integration and security event automation pipelines

Company Description