# Architectural Decisions

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID: | Subject: | Issue / Requirement: | Decision: | Rationale: | Source: Project Phase: |
| G01 | Cost Efficiency | GCP projects managed independently by departments risk duplicated services, inefficient spending, and lack of consolidated cost tracking. Require cost allocation, tagging strategies, and budget control mechanisms. | Implement GCP Resource Hierarchy with centralized billing account and per-department projects. Enable cost tracking using labels and cost controls with Budget and Alert policies. | Allows cost visibility, optimization, and billing transparency across departments while preserving autonomy. |  |
| G02 | Security & Compliance | Managing IAM policies and compliance for regulated workloads (e.g., Kronos with PII) requires centralized controls and monitoring. Departments need flexibility without compromising governance. | Use GCP Organization policies and IAM Conditions with central logging via Cloud Audit Logs and SCC. | Provides centralized control, fine-grained permissions, and compliance visibility for sensitive workloads. |  |
| G03 | Workload Isolation | Departments require isolated compute and network environments for development, testing, and production. Need to enforce environment separation while allowing shared service access. | Use GCP folders and projects per environment per department with Shared VPC and Service Perimeters. | Enables secure, scalable, and isolated environments with controlled interconnectivity. |  |
| G04 | Operational Efficiency | Manual environment setup causes inconsistency and delays. Require automated provisioning, consistency, and drift detection. | Adopt Terraform with CI/CD pipelines, standard modules, and policies-as-code using OPA or Forseti. | Delivers automation, compliance, and reduced operational effort across multi-team environments. |  |
| G05 | Networking and Connectivity | Need centralized control over VPN, DNS, and NAT services while enabling scalable interconnectivity. | Implement hub-and-spoke networking with Shared VPC in the hub and spoke VPCs per department. | Reduces network complexity and centralizes control, monitoring, and security. |  |