GCP Cloud Infrastructure – Consolidated Implementation Plan

# Overview

This effort involves reviewing and improving GCP project structure, access control, logging, monitoring, network architecture, and security integrations to align with best practices and improve cloud governance, visibility, and posture.

# Recommendations & Benefits

|  |  |  |
| --- | --- | --- |
| Recommendation | Description | Benefit |
| Project Structure | Review current structure and make necessary adjustments to folders and projects. | Enables better organization, billing, and access segregation. |
| Naming Convention | Standardize naming for folders/projects/resources. | Improves discoverability and operational clarity. |
| Identity & Access Mgmt | Integrate with Azure AD and enforce least privilege access. | Centralized user management and improved security posture. |
| Network Architecture | Implement hub-and-spoke model with firewalls, NAT, and Cloud Armor. | Scalable and secure network model. |
| Logging & Monitoring | Enable logs for all services, integrate with Splunk and setup alerting. | Centralized visibility and operational observability. |
| Security & Compliance | Adopt security best practices and integrate with Wiz.io. | Stronger vulnerability detection and regulatory alignment. |

# Milestones / Deliverables

|  |  |
| --- | --- |
| Task | Deliverable |
| Project Structure & Naming | Document GCP hierarchy and apply naming standards. |
| Centralized Identity Mgmt | Review identity setup and Azure AD federation. |
| Identity User List Review | Audit current user roles and enforce least privilege. |
| Firewall Rules Audit | Validate all ingress/egress rules across VPCs. |
| Logging Integration | Ensure logs are pushed to Splunk and metrics/alerts configured. |

# Dependencies

|  |  |
| --- | --- |
| Dependency | Required Action |
| Project Structure Review | Extract current project/folder layout and approve naming standards. |
| Identity Details | Review Azure AD groups, roles, and mappings. |
| Firewall Config Access | Access firewall rule documentation and export list. |
| Splunk Access | Verify log forwarding and alert rules in the Splunk portal. |

# High-Level Timeline (Monthly Milestones)

|  |  |  |
| --- | --- | --- |
| Month | Milestone | Description |
| Month 1 | Project Setup & IAM Design | Create folders, projects, billing, and IAM role definitions. |
| Month 2 | Networking & Security Foundation | VPC, subnets, firewall, Cloud NAT, Cloud Armor deployment. |
| Month 3 | Resource Provisioning Automation | Use Terraform/Deployment Manager to automate provisioning. |
| Month 4 | Monitoring, Logging & Alerting | Set up Logging, Monitoring, Splunk forwarding, alert policies. |
| Month 5 | CI/CD and App Deployments | Configure Cloud Build/GitLab CI, GKE/Cloud Run deployments. |
| Month 6 | Governance & Optimization | Apply labels/tags, audit permissions, optimize costs & performance. |