1. GCP Project Milestones (High-Level Plan)

Timeline Milestone Description

Month 1 Project Setup & IAM Design Set up GCP organization/project structure, folders, billing, and IAM roles

Month 2 Networking & Security Foundation VPC setup, subnets, firewall rules, Cloud NAT, and Cloud Armor

Month 3 Resource Provisioning Automation Use Terraform/Deployment Manager for repeatable infra provisioning

Month 4 Monitoring, Logging & Alerting Enable Cloud Monitoring, Logging, Error Reporting, custom metrics

Month 5 CI/CD and Application Deployments Cloud Build/GitLab CI integration, Artifact Registry, GKE or Cloud Run

Month 6 Governance & Optimization Cost analysis, security audits, labels/tags, and performance optimization

🧩 Key Real-Time Scenarios & Examples

Scenario 1: IAM Misconfiguration

Issue: Broad access granted (e.g., roles/editor to a user).

Action: Implement least privilege principle using custom roles.

Example: A developer only needs access to GCS; assign roles/storage.objectViewer instead of Editor.

Scenario 2: Resource Sprawl and Naming Confusion

Issue: Hard to track resources in shared environments.

Action: Apply consistent naming conventions and labels.

Example: gke-dev-cluster-us-west1 or vm-prod-billing-app-us-central1

Scenario 3: Inconsistent Monitoring

Issue: No unified alerting or dashboard.

Action: Set up Cloud Monitoring Dashboards with uptime checks and SLOs.

Example: Monitor GKE pods, API latency, VM CPU usage.

Scenario 4: Manual Provisioning Delays

Issue: Environment setup takes time across teams.

Action: Automate using Terraform modules with standardized naming and variables.

Example: Automate Cloud SQL setup with backup configs, IAM, and alerting.

1. Naming Standards

Resource Type Format Example

GCS Bucket env-appname-purpose-region → dev-billing-data-us

VM Instances env-appname-tier-location → prod-web-frontend-usw1

Pub/Sub env-topicname → stg-orders-topic

GKE Cluster env-cluster-region → dev-cluster-usw1

2. Annotations, Labels, and Tags

Use labels for billing, team ownership, and lifecycle:

yaml

Copy

Edit

labels:

environment: dev

team: analytics

cost-center: 1234

owner: madhu

Enforce organization policies to mandate labels during resource creation.

🔷 3. Standards & Governance

Define Terraform modules for consistent resource creation.

Enforce Cloud Asset Inventory and Config Validator for policy compliance.

Enable GCP Organization Policy Constraints (e.g., disable external IPs on VMs).

Conduct bi-weekly FinOps reviews for cost anomalies.

🛠 Tools You Can Drive

Terraform: Infrastructure-as-code for GCP provisioning

Cloud Build + GitHub/GitLab CI: CI/CD pipelines

Cloud Monitoring + Dashboards: Visibility

Security Command Center: Risk management

BigQuery Audit Log Analysis: User access and usage tracking