**Project Name:** GCP Cloud Infrastructure Security Enhancement & Standardization  
**Project Owner:** [To be filled by user]  
**Duration:** Q4 2025 to Q4 2026  
**Scope:** Standardizing GCP infrastructure with secure access, naming conventions, controlled environments, and centralized identity and policy enforcement.

**1. Overview**

This initiative focuses on modernizing and securing the GCP infrastructure. It includes the standardization of resource naming, access control, logging, and implementing best practices for firewall and identity management.

**2. Milestones and Deliverables**

**Q4 2025:**

* **Assessment Phase**
  + Capture current GCP state: projects, users, firewall rules, and IAM policies.
  + Identify gaps in naming conventions, identity management, and logging.
  + Document current vs. target state.
* **Cost Analysis**
  + Analyze existing resources and usage.
  + Recommend optimization to reduce costs.

**Q1 2026:**

* **Naming Convention Implementation**
  + Define and apply consistent project/folder/resource naming standards.
  + Apply naming convention to all existing and new projects.
* **Firewall & IP Management**
  + Review and restructure firewall rules.
  + Assign fixed IPs to controlled environments (Dev, QA, Prod).
  + Document ingress/egress policies.

**Q2 2026:**

* **Centralized Identity and Access Management**
  + Integrate GCP IAM with centralized AD/SSO.
  + Define least privilege roles and implement access review policies.
  + Apply RBAC to GCP folders and resources.
* **Policy Enforcement**
  + Develop organization policies for resource creation (e.g., labels, tags).
  + Prevent direct IAM changes at project level.

**Q3 2026:**

* **Logging & Monitoring**
  + Ensure all logs are forwarded to Splunk.
  + Enable audit logs across all projects.
  + Define alert policies for critical events.
* **Security Integration**
  + Integrate GCP with Wiz.io for security posture management.
  + Enable vulnerability detection and remediation workflows.

**Q4 2026:**

* **Final Review and Handoff**
  + Validate the implemented changes against the target state.
  + Handoff documentation, SOPs, and access control list to ops team.

**3. Dependencies**

* Approval of project naming standards.
* Centralized Identity Management system access (e.g., Azure AD).
* Splunk access for log verification.
* Firewall rule export and approval for changes.

**4. Recommendations**

* Revisit and revise network architecture if required (Hub-and-Spoke model).
* Enforce mandatory tagging policies.
* Apply VPC Service Controls for high-risk services.
* Enable security command center and cloud DLP.

**5. Security Objectives**

* Enforce Least Privilege principle across all services.
* Protect access using IAM Conditions and MFA.
* Implement policy constraints (e.g., disallow public IP).
* Enable secure image policies for compute.
* Apply encryption policies for storage and secrets.

**6. Benefits**

* **Enhanced Security**: Reduced attack surface and improved threat response.
* **Operational Efficiency**: Easier resource discovery and automation.
* **Governance**: Policy and access controls applied consistently.
* **Compliance**: Supports HIPAA, GDPR, and internal audit readiness.

**7. Key Tools and Integrations**

* **Splunk**: For centralized logging and monitoring.
* **Wiz.io**: Security posture and vulnerability scanning.
* **GCP IAM**: Role-based access control.
* **Cloud Monitoring & Logging**: Native GCP observability tools.

**8. Team Roles**

* **Cloud Architect**: Define target architecture, security enforcement.
* **IAM Engineer**: Implement access control, directory sync.
* **DevOps**: Apply CI/CD pipelines for policy and firewall rules.
* **Security Analyst**: Integrate Wiz.io and analyze vulnerability trends.