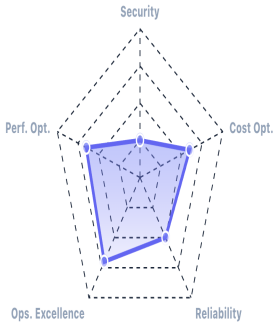
Readiness Audit Report

GENERATED: 22.12.2025, 07:07:55 | GCP ARCHITECTURE FRAMEWORK AUDIT

Executive Summary

Audit reveals critical security vulnerabilities including an unrestricted firewall allowing global ingress and public IP exposure on compute instances. Significant cost inefficiencies identified in storage provisioning and legacy compute types. Immediate remediation required for compliance with CIS GCP and NIST standards.



Detailed Infrastructure Assessment

Severity / Pillar	Context	Finding Details
CRITICAL Security	main.tf Line 13	UNRESTRICTED FIREWALL INGRESS (0.0.0.0/0) The firewall rule allows ingress from any IP address on the internet to all ports (0-65535), exposing the network to scanning, brute force, and exploitation. ACTION: Restrict source ranges to specific trusted IPs or internal CIDR blocks and limit ports to necessary services only.
HIGH Security	main.tf Line 38	PUBLIC IP ADDRESS ASSIGNMENT The compute instance is configured with an ephemeral public IP address via the empty `access_config` block, bypassing the need for a bastion or VPN. ACTION: Remove the `access_config` block to ensure the instance only has a private IP. Use Cloud NAT for outbound access if needed.
HIGH Security	main.tf Line 6	UNIFORM BUCKET LEVEL ACCESS DISABLED The storage bucket allows legacy ACLs (Access Control Lists), which can lead to inconsistent permission management and accidental public exposure. ACTION: Enable Uniform Bucket Level Access to centralize permission management via IAM.
MEDIUM Cost Optimization	main.tf Line 44 Save ~$65.00/mo (Switching 500GB from SSD to Standard)	EXPENSIVE STORAGE CLASS FOR BACKUP A 500GB PD-SSD disk is provisioned for what appears to be a backup/unused resource. SSDs are significantly more expensive than Standard Persistent Disks. ACTION: Downgrade the disk type to `pd-standard` or `pd-balanced` for backup workloads.
MEDIUM Cost Optimization	main.tf Line 27 ~15-20% compute savings + performance gain	LEGACY MACHINE TYPE USAGE The `n1-standard-1` machine type is a legacy generation. Newer generations like E2 or N2 offer better price-performance ratios. ACTION: Update the machine type to `e2-standard-2` or `e2-medium` depending on load requirements.
MEDIUM Reliability	main.tf Line 9	STORAGE OBJECT VERSIONING DISABLED Versioning is explicitly disabled on a production bucket, making it impossible to recover overwritten or deleted objects. ACTION: Enable object versioning to support data recovery and audit trails.

Severity / Pillar	Context	Finding Details
HIGH Operational Excellence	main.tf Line 4	FORCE DESTROY ENABLED ON PRODUCTION The `force_destroy` attribute allows Terraform to delete the bucket even if it contains data, posing a severe risk to production data. ACTION: Set `force_destroy` to `false` for production environments to prevent accidental data loss.