



INFRASTRUCTURE AUDIT REPORT

Deployment Readiness Assessment Protocol v2.5

REPORT ID: DRA-06046486

DATE: 22/12/2025

PROPRIETARY & CONFIDENTIAL

This document contains proprietary architectural analysis. Unauthorized distribution is prohibited.



Executive Summary

Architectural Integrity Analysis & Risk Profiling

1. Overall Readiness Summary

The audit reveals critical security vulnerabilities and significant cost inefficiencies. The most urgent issues are the unrestricted firewall rule allowing global access to all ports and the exposure of the compute instance via a public IP with a privileged default service account. Storage configurations lack essential data protection mechanisms (versioning, uniform access). Cost optimization opportunities exist by modernizing machine types and rightsizing storage disks.

2. Pillar Performance Assessment

Architecture Pillar	Score	Status	Auditor Analysis
SECURITY	15/100	Critical	Found unrestricted firewall rules (0.0.0.0/0), public IP assignment, use of default service accounts with excessive privileges, and weak storage IAM settings.
COST OPTIMIZATION	60/100	Warning	Legacy N1 machine types and expensive SSDs used for backup purposes indicate wasted spend.
RELIABILITY	50/100	Warning	Data loss risks identified: Bucket versioning is disabled and 'force_destroy' is enabled on production data.

ARCHITECTURE PILLAR	SCORE	STATUS	AUDITOR ANALYSIS
OPERATIONAL EXCELLENCE	40/100	WARNING	Resources lack labels for billing/management and logging is not explicitly enabled for buckets or firewalls.
PERFORMANCE	70/100	SAFE	While N1 is older, it is functional, though E2/N2 would offer better price-performance.

3. Technical Observation Log

SEVERITY	CONTEXT	FINDING, REMEDIATION & COMPLIANCE
CRITICAL	SOURCE: main.tf LOCATION: Line 13 CATEGORY: Security	<p>UNRESTRICTED FIREWALL INGRESS (0.0.0.0/0)</p> <p>The firewall rule 'allow_all' permits ingress traffic on all ports (0-65535) from the entire internet (0.0.0.0/0). This exposes the network to scanning, brute force, and exploitation attacks.</p> <p>REMEDIATION STRATEGY: Restrict source ranges to specific trusted IPs or internal subnets. Only allow necessary ports (e.g., 443 for web, 22 for SSH via IAP).</p> <p>COMPLIANCE MAPPING:</p> <ul style="list-style-type: none">• CIS GCP Benchmark: 3.6• PCI DSS: 1.2.1 <p>RECOMMENDED HCL FIX:</p> <pre>----- resource "google_compute_firewall" "allow_specific" { name = "allow-web-ingress" network = "default" allow { protocol = "tcp" ports = ["443"] } source_ranges = ["10.0.0.0/8"] # Example internal range }</pre> <p>-----</p>
HIGH	SOURCE: main.tf LOCATION: Line 38 CATEGORY: Security	<p>PUBLIC IP ADDRESS ASSIGNED TO VM</p> <p>The instance 'legacy_server' is assigned a public IP address via the 'access_config' block. This increases the attack surface significantly.</p> <p>REMEDIATION STRATEGY: Remove the 'access_config' block. Use Identity-Aware Proxy (IAP) for SSH access and Cloud NAT for outbound internet access.</p> <p>COMPLIANCE MAPPING:</p>

Severity	Context	Finding, Remediation & Compliance
		<ul style="list-style-type: none"> • NIST 800-53: AC-3 <p>RECOMMENDED HCL FIX:</p> <pre>----- network_interface { network = "default" # access_config {} <-- Removed to prevent public IP } -----</pre>
CRITICAL	<p>SOURCE: <i>main.tf</i> LOCATION: Line 25 CATEGORY: Security</p>	<p>DEFAULT SERVICE ACCOUNT USED</p> <p>The VM instance does not specify a 'service_account' block, causing it to use the default Compute Engine service account which has the primitive 'Editor' role project-wide.</p> <p>REMEDIATION STRATEGY: Create a custom service account with least-privilege IAM roles and assign it to the instance.</p> <p>COMPLIANCE MAPPING:</p> <ul style="list-style-type: none"> • CIS GCP Benchmark: 4.1 <p>RECOMMENDED HCL FIX:</p> <pre>----- resource "google_service_account" "app_sa" { account_id = "app-sa" } resource "google_compute_instance" "legacy_server" { # ... service_account { email = google_service_account.app_sa.email scopes = ["cloud-platform"] } }</pre>
HIGH	<p>SOURCE: <i>main.tf</i> LOCATION: Line 6 CATEGORY: Security</p>	<p>UNIFORM BUCKET LEVEL ACCESS DISABLED</p> <p>The bucket 'corporate_data' has 'uniform_bucket_level_access' set to false, allowing object-level ACLs which are difficult</p>

Severity	Context	Finding, Remediation & Compliance
Medium	<p>SOURCE: <i>main.tf</i> LOCATION: Line 9 CATEGORY: Reliability</p>	<p>to manage and audit.</p> <p>REMEDIATION STRATEGY: Set 'uniform_bucket_level_access' to true to enforce IAM policies at the bucket level.</p> <p>COMPLIANCE MAPPING:</p> <ul style="list-style-type: none"> CIS GCP Benchmark: 5.2 <p>RECOMMENDED HCL FIX:</p> <pre>----- resource "google_storage_bucket" "corporate_data" { # ... uniform_bucket_level_access = true } -----</pre>
Medium	<p>SOURCE: <i>main.tf</i> LOCATION: Line 9 CATEGORY: Reliability</p>	<p>BUCKET VERSIONING DISABLED</p> <p>Versioning is explicitly disabled for 'corporate_data'. Accidental overwrites or deletions cannot be recovered.</p> <p>REMEDIATION STRATEGY: Enable object versioning to protect data integrity.</p> <p>COMPLIANCE MAPPING:</p> <ul style="list-style-type: none"> NIST 800-53: CP-9 <p>RECOMMENDED HCL FIX:</p> <pre>----- versioning { enabled = true } -----</pre>
Medium	<p>SOURCE: <i>main.tf</i> LOCATION: Line 4 CATEGORY: Reliability</p>	<p>FORCE DESTROY ENABLED ON PRODUCTION BUCKET</p> <p>The 'force_destroy' attribute is set to true. Terraform will delete the bucket and all its contents without error if the resource is removed from code, posing a severe data loss risk.</p> <p>REMEDIATION STRATEGY: Set 'force_destroy' to false for production environments.</p>

SEVERITY	CONTEXT	FINDING, REMEDIATION & COMPLIANCE
		<p>COMPLIANCE MAPPING:</p> <ul style="list-style-type: none"> • Operational Best Practice: N/A <p>RECOMMENDED HCL FIX:</p> <pre>----- resource "google_storage_bucket" "corporate_data" { # ... force_destroy = false } -----</pre>
MEDIUM	<p>SOURCE: <i>main.tf</i> LOCATION: Line 44 CATEGORY: Cost Optimization</p>	<p>EXPENSIVE DISK TYPE FOR BACKUP</p> <p>The disk 'unattached_disk' uses 'pd-ssd' (SSD Persistent Disk) but is named 'unused-disk-backup'. SSDs are significantly more expensive than Standard or Balanced disks and unnecessary for cold backups.</p> <p>REMEDIATION STRATEGY: Change the disk type to 'pd-standard' or 'pd-balanced'.</p> <p>COMPLIANCE MAPPING:</p> <ul style="list-style-type: none"> • Cost Optimization: N/A <p>RECOMMENDED HCL FIX:</p> <pre>----- resource "google_compute_disk" "unattached_disk" { # ... type = "pd-standard" } -----</pre>
LOW	<p>SOURCE: <i>main.tf</i> LOCATION: Line 27 CATEGORY: Performance</p>	<p>LEGACY MACHINE TYPE USED</p> <p>The instance uses 'n1-standard-1', a first-generation machine type. Newer generations like E2 or N2 offer better price-performance ratios.</p> <p>REMEDIATION STRATEGY: Upgrade to 'e2-standard-2' (balanced) or 'n2-standard-2'.</p> <p>COMPLIANCE MAPPING:</p> <ul style="list-style-type: none"> • Performance Efficiency: N/A <p>RECOMMENDED HCL FIX:</p> <pre>-----</pre>

SEVERITY	CONTEXT	FINDING, REMEDIATION & COMPLIANCE
LOW	<p>SOURCE: <i>main.tf</i> LOCATION: Line 25 CATEGORY: <i>Operational Excellence</i></p>	<pre>resource "google_compute_instance" "legacy_server" { # ... machine_type = "e2-medium" # or e2-standard-2 depending on load }</pre> <hr/> <p>MISSING RESOURCE LABELS</p> <p>Resources (Bucket, Instance, Disk) lack labels. Labels are essential for cost allocation, filtering, and ownership tracking.</p> <p>REMEDIATION STRATEGY: Add a 'labels' block to all resources defining environment, owner, and cost center.</p> <p>COMPLIANCE MAPPING:</p> <ul style="list-style-type: none"> • Google Cloud Architecture Framework: Cost Management <p>RECOMMENDED HCL FIX:</p> <hr/> <pre>resource "google_compute_instance" "legacy_server" { # ... labels = { environment = "prod" team = "legacy-ops" cost_center = "1234" } }</pre> <hr/>
MEDIUM	<p>SOURCE: <i>main.tf</i> LOCATION: Line 25 CATEGORY: Security</p>	<p>SHIELDED VM CONFIG MISSING</p> <p>The compute instance does not have Shielded VM features (Secure Boot, vTPM, Integrity Monitoring) enabled.</p> <p>REMEDIATION STRATEGY: Add the 'shielded_instance_config' block and enable secure boot.</p> <p>COMPLIANCE MAPPING:</p> <ul style="list-style-type: none"> • CIS GCP Benchmark: 4.4 <p>RECOMMENDED HCL FIX:</p> <hr/>

SEVERITY	CONTEXT	FINDING, REMEDIATION & COMPLIANCE
----------	---------	-----------------------------------

```
resource "google_compute_instance" "legacy_server" {
  # ...
  shielded_instance_config {
    enable_secure_boot = true
    enable_vtpm       = true
    enable_integrity_monitoring = true
  }
}
```
