SAMPLE REPORT · DEMO DATA

# Cloud Controls Findings

Acme Corp


PREPARED BY

**Musah Abdulai**

Cloud controls & security-review implementation

Google Cloud Professional DevOps Engineer


May 21, 2026 · musabdulai.com

⚠ **Demo data** — illustrative findings for a fictional B2B SaaS company. This report shows the format and depth of a real Controls Review deliverable. Numbers, systems, and account names are made up.

SAMPLE REPORT

# Cloud controls findings — Acme Corp

Output of a 48-hour Controls Review across IAM, logging, CI/CD, vulnerability, backup, and AI workload controls for a fictional Series B SaaS company.

| | |
|---|---|
| **ENGAGEMENT** | **SCOPE** |
| Controls Review · 48 hours | AWS, GCP, GitHub, Vanta, Vertex AI |
| **TRIGGER** | **FINDINGS** |
| Enterprise security review | HIGH 3 MEDIUM 5 LOW 1 |

## Executive summary

Acme Corp has the foundations of a working cloud and engineering setup, but a customer security review will surface concrete gaps in logging, IAM hygiene, deploy approvals, backup evidence, and AI cost control. None of the findings require a re-architecture. All can be implemented inside a 1–2 week Controls Sprint with merged PRs and an evidence folder ready to share with the enterprise buyer's procurement team.

The highest-impact moves are: enabling org-wide CloudTrail, retiring long-lived service-account keys via Workload Identity, and enforcing MFA + deploy approvals as policy. These three changes alone cover the majority of items a SOC 2 readiness assessment or customer questionnaire will flag.

# Findings

## F-01 CloudTrail not enabled in 2 of 3 production accounts

HIGH

**AREA**

Logging & monitoring

**AFFECTED SYSTEM**

`AWS / CloudTrail`

**OWNER**

Platform / Security

**ESTIMATE**

1-2 days

**BUYER / AUDIT RELEVANCE**

Auditors and enterprise buyers expect a complete audit trail across all production accounts. Missing CloudTrail in any production account blocks SOC 2 CC7.2 evidence.

**EVIDENCE REQUESTED**

Org-level CloudTrail config export · per-account trail status screenshots.

**FIX PATH**

Create org-wide CloudTrail in management account; ship logs to dedicated security S3 bucket with object-lock; enable log-file validation.

## F–02 Service-account keys not rotated in 11+ months

HIGH

**AREA**

Access controls

**AFFECTED SYSTEM**

`GCP / IAM`

**OWNER**

Platform

**ESTIMATE**

3-5 days

**BUYER / AUDIT RELEVANCE**

Stale long-lived keys are a top finding on customer questionnaires and Vanta/Drata IAM checks.

**EVIDENCE REQUESTED**

gcloud IAM keys inventory · documented rotation policy · IaC change history.

**FIX PATH**

Migrate service-to-service auth to Workload Identity; revoke long-lived JSON keys; document rotation policy and quarterly review.

## F-03 No required reviews on production deploy workflow

MEDIUM

**AREA**

CI/CD & change management

**AFFECTED SYSTEM**

`GitHub Actions`

**OWNER**

Engineering Leads

**ESTIMATE**

0.5-1 day

**BUYER / AUDIT RELEVANCE**

Customer questionnaires routinely ask for evidence of code-review and deployment approval gates (SOC 2 CC8.1).

**EVIDENCE REQUESTED**

Branch-protection JSON export · CODEOWNERS file · GitHub environment protection screenshot.

**FIX PATH**

Enable required PR reviews and required status checks on main; gate production environment on a designated approvers group.

## F–04 Container images deployed without scanning

MEDIUM

**AREA**

Vulnerability hygiene

**AFFECTED SYSTEM**

`Artifact Registry / CI`

**OWNER**

Platform

**ESTIMATE**

1 day

**BUYER / AUDIT RELEVANCE**

Vanta and Drata both flag missing image scanning. Enterprise buyers ask for evidence that no critical/high CVEs are deployed.

**EVIDENCE REQUESTED**

CI pipeline log showing scan step · scanner output for last 30 deploys · policy doc.

**FIX PATH**

Add Trivy or Artifact Registry vulnerability scanning to CI; fail builds on critical CVEs; document exception process.

## F-05 Database backups: no documented restore test

MEDIUM

**AREA**

Backups & recovery

**AFFECTED SYSTEM**

`Cloud SQL / RDS`

**OWNER**

Platform / SRE

**ESTIMATE**

1-2 days

**BUYER / AUDIT RELEVANCE**

Restore tests (not just backup configuration) are the evidence auditors and buyers actually want.

**EVIDENCE REQUESTED**

Restore-test runbook · last restore-test report · monitoring of backup success.

**FIX PATH**

Document quarterly restore-test runbook; schedule a recurring drill; capture restored row counts and runtime in the evidence folder.

## F–06 Admin console access lacks enforced MFA evidence

HIGH

**AREA**

Access controls

**AFFECTED SYSTEM**

`Identity provider (Okta / Google Workspace)`

**OWNER**

IT / Security

**ESTIMATE**

0.5-1 day

**BUYER / AUDIT RELEVANCE**

MFA evidence is the single most-requested item on customer security questionnaires.

**EVIDENCE REQUESTED**

IdP policy export · per-user MFA status report · enforcement screenshot.

**FIX PATH**

Set IdP policy to require MFA for all admin roles; revoke standing access for users without MFA; export quarterly evidence.

## F–07 AI feature has no token-spend guardrail

MEDIUM

**AREA**

AI workload controls

**AFFECTED SYSTEM**

`Vertex AI / OpenAI`

**OWNER**

AI / Platform

**ESTIMATE**

1-2 days

**BUYER / AUDIT RELEVANCE**

Procurement teams increasingly ask whether AI features can be rate-limited and have cost controls before granting enterprise access.

**EVIDENCE REQUESTED**

Spend dashboard · per-tenant rate-limit policy · alert routing config.

**FIX PATH**

Set per-tenant token quotas; route spend alerts to on-call; document abuse-handling runbook.

## F–08 No documented offboarding evidence for terminated users

MEDIUM

**AREA**

Access controls

**AFFECTED SYSTEM**

`IdP / Cloud / Git`

**OWNER**

HR / IT

**ESTIMATE**

0.5-1 day

**BUYER / AUDIT RELEVANCE**

Auditors expect time-bound evidence that access was revoked across all systems for departed users.

**EVIDENCE REQUESTED**

Offboarding checklist · ticket history for last 5 offboardings · IdP audit export.

**FIX PATH**

Document offboarding runbook with checkpoints across IdP, cloud, repo, and SaaS; store completed checklists in evidence folder.

### F-09 Secret scanning not enabled on repositories

LOW

**AREA**

Vulnerability hygiene

**AFFECTED SYSTEM**

`GitHub`

**OWNER**

Security

**ESTIMATE**

0.5 day

**BUYER / AUDIT RELEVANCE**

Secret scanning is an easy check that customer questionnaires often ask about explicitly.

**EVIDENCE REQUESTED**

Repo settings screenshot · secret scanning alert dashboard · remediation history.

**FIX PATH**

Enable GitHub Advanced Security secret scanning org-wide; route alerts to a security channel; document triage SLA.

NEXT STEPS

## About this report

Prepared by Musah Abdulai, a cloud controls implementation engineer for B2B SaaS and AI-product teams. This sample demonstrates the depth and format of a real Controls Review deliverable. To see whether a fixed-scope review can fix the gaps a customer security review will surface for your stack, book a 15-minute fit call or reach out directly.

Book a controls review →

or email **hello@musabdulai.com**