



CLOUD & SECURITY AUDIT

# Audit Report

Cloud architecture, CI/CD, access, AI agents, monitoring and compliance readiness

**SAMPLE REPORT** Company details are changed. Findings are representative of a typical audit.

|              |                                                                                                                                   |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Prepared for | Sample Co. (US fintech, about 80 people, payments platform)                                                                       |
| Environment  | AWS, two accounts (production and staging), 14 services, GitHub Actions CI/CD                                                     |
| Reviewed by  | Lokesh Kojhani, Security Architect, CISSP, CSSLP                                                                                  |
| Method       | 60-minute call with the engineering lead, read-only access to the cloud account and repositories, review of policies and alerting |
| Report date  | Written report delivered within 5 business days of the call                                                                       |

*This report is confidential to the client it was written for. The version you are reading is a sample with company details changed, shared so teams can see what a Triotech audit delivers.*

1. SUMMARY

What we found

Sample Co. runs a clean, well-documented platform for its size. The main risks come from fast growth: access that was set up for a five-person team is now used by forty engineers and an AI coding agent, and cloud costs have grown faster than traffic.

3

High-risk findings to fix first

6

Medium-risk findings

7

Quick wins you can fix this week

\$4,800

Estimated monthly cloud savings (about 18%)

Score by area

| Area                                 | Risk   | Main finding                                                                                |
|--------------------------------------|--------|---------------------------------------------------------------------------------------------|
| Cloud architecture & cost            | Medium | Healthy layout, but 11 servers run under 15% load and old snapshots are still billed.       |
| CI/CD & secrets                      | High   | The pipeline deploys with a long-lived admin key stored as a repository secret.             |
| Access & IAM                         | High   | 2 of 5 admin users have no MFA, and nobody reviews access on a schedule.                    |
| AI agent permissions                 | High   | The AI coding agent uses a personal token that can change CI workflows in every repository. |
| Monitoring & incident response       | Medium | Alerts go to a shared inbox. Nothing pages anyone outside business hours.                   |
| SOC 2, HIPAA, PIPEDA, GDPR readiness | Medium | Logs are kept for 7 days, short of what an auditor will ask to see.                         |

## 2. FINDINGS

## Risks ranked High, Medium, Low

Each finding shows why it matters and the fix we recommend, with a rough effort so you can plan. Fix the high-risk items first.

| ID | Risk   | Finding and why it matters                                                                                                                                                | Recommended fix                                                                                                                                    | Effort      |
|----|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| H1 | High   | <b>Pipeline deploys with a long-lived admin key</b><br>Anyone who gets this key, from a leaked log or a compromised workflow, gets full control of production.            | Switch the pipeline to short-lived role credentials (OIDC). Limit the role to what each deploy needs. Delete the old key.                          | 1 to 2 days |
| H2 | High   | <b>Admin users without MFA</b><br>2 of 5 admin accounts can sign in with a password alone. One of them belongs to a former contractor.                                    | Turn on MFA for every admin. Remove the contractor account. Move admins to single sign-on.                                                         | 2 hours     |
| H3 | High   | <b>AI coding agent has broad write access</b><br>The agent runs on a senior engineer's personal token. It can edit CI workflows and merge to main in all 38 repositories. | Give the agent its own identity, limit it to the repositories it works in, block edits to workflow files, and require a human review before merge. | 1 day       |
| M1 | Medium | <b>Secrets stored in service environment variables</b><br>3 services keep database and API secrets in plain environment variables with no rotation.                       | Move them to a secrets manager and rotate every 90 days.                                                                                           | 2 days      |
| M2 | Medium | <b>No out-of-hours alerting</b><br>Alerts go to a shared inbox. A problem at 2 AM waits until someone checks email.                                                       | Route critical alerts to an on-call rotation with paging. Write a one-page response guide.                                                         | 1 day       |
| M3 | Medium | <b>Backups never restore-tested</b><br>Database backups run nightly, but nobody has tried a full restore.                                                                 | Run a restore test this quarter and then every 6 months. Record how long it takes.                                                                 | 1 day       |
| M4 | Medium | <b>Oversized servers</b><br>11 servers averaged under 15% CPU over the last 30 days.                                                                                      | Right-size them in two batches and watch load for a week after each.                                                                               | 2 days      |
| M5 | Medium | <b>Log retention too short for an audit</b><br>Logs are kept for 7 days. A SOC 2 auditor will ask for evidence across the whole audit period.                             | Keep 90 days searchable and 1 year in low-cost archive storage.                                                                                    | 4 hours     |
| M6 | Medium | <b>Main branch unprotected in 4 repositories</b><br>Changes can reach production without a review.                                                                        | Require pull requests, one approval and passing checks on main in every repository.                                                                | 2 hours     |
| L1 | Low    | <b>Unused storage still billed</b><br>Detached volumes and snapshots older than 6 months cost about \$620 a month.                                                        | Delete them after a final check, and add a monthly cleanup rule.                                                                                   | 2 hours     |
| L2 | Low    | <b>Missing security headers on the admin app</b><br>Makes some browser-based attacks easier.                                                                              | Add the standard set of security headers.                                                                                                          | 2 hours     |
| L3 | Low    | <b>No cost tags</b><br>Spend cannot be split by team or service.                                                                                                          | Add a tagging policy and enforce it on new resources.                                                                                              | 1 day       |

| ID | Risk | Finding and why it matters                                                                   | Recommended fix                                    | Effort            |
|----|------|----------------------------------------------------------------------------------------------|----------------------------------------------------|-------------------|
| L4 | Low  | <b>Access reviews not documented</b><br>Auditors will ask for proof that access is reviewed. | Run a quarterly access review and keep the record. | 2 hours a quarter |

3. QUICK WINS

Fix these this week

| # | Quick win                                                                              | Time    |
|---|----------------------------------------------------------------------------------------|---------|
| 1 | Turn on MFA for every admin and remove the former contractor's account (H2)            | 2 hours |
| 2 | Protect the main branch in the 4 open repositories (M6)                                | 2 hours |
| 3 | Limit the AI agent's token to the repositories it actually works in (first step of H3) | 1 hour  |
| 4 | Delete unused volumes and old snapshots (L1), saving about \$620 a month               | 2 hours |
| 5 | Extend log retention to 90 days (M5)                                                   | 1 hour  |
| 6 | Send critical alerts to a paging tool instead of the shared inbox (first step of M2)   | 2 hours |
| 7 | Add security headers to the admin app (L2)                                             | 2 hours |

CLOUD COST

Where the \$4,800 a month comes from

| Change                                                      | Monthly saving | Effort  |
|-------------------------------------------------------------|----------------|---------|
| Right-size 11 underused servers (M4)                        | \$2,300        | 2 days  |
| Commit to a 1-year savings plan for steady workloads        | \$1,600        | 2 hours |
| Remove unused storage and old snapshots (L1)                | \$620          | 2 hours |
| Move older logs to archive storage (M5)                     | \$280          | 4 hours |
| <b>Total, from a current bill of about \$26,500 a month</b> | <b>\$4,800</b> |         |

## 4. 90-DAY ROADMAP

## The bigger fixes, in order

|                                             |                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Days 1 to 30</b><br>Close the high risks | <ul style="list-style-type: none"><li>• Pipeline moved to short-lived credentials, old admin key deleted (H1)</li><li>• AI agent on its own identity with limited access and required review (H3)</li><li>• Single sign-on for all admins (H2)</li><li>• Critical alerts paging an on-call rotation (M2)</li></ul> |
| <b>Days 31 to 60</b><br>Harden and save     | <ul style="list-style-type: none"><li>• Secrets moved to a secrets manager with rotation (M1)</li><li>• Servers right-sized and savings plan in place (M4)</li><li>• First full backup restore test (M3)</li><li>• Cost tagging policy live (L3)</li></ul>                                                         |
| <b>Days 61 to 90</b><br>Get audit-ready     | <ul style="list-style-type: none"><li>• 90-day log retention and 1-year archive confirmed (M5)</li><li>• First quarterly access review recorded (L4)</li><li>• Short incident response guide and one practice run</li><li>• Re-check of all findings and an updated score by area</li></ul>                        |

## COMPLIANCE READINESS

## Where Sample Co. stands for a first SOC 2 audit

| Control area           | Status   | What is missing                                           |
|------------------------|----------|-----------------------------------------------------------|
| Access control         | Partial  | MFA gaps and no access reviews (H2, L4)                   |
| Change management      | Partial  | Unprotected branches in 4 repositories (M6)               |
| Logging and monitoring | Gap      | Short log retention and no out-of-hours alerting (M2, M5) |
| Backup and recovery    | Partial  | Restores never tested (M3)                                |
| Encryption             | In place | Data encrypted at rest and in transit                     |

## 5. NEXT STEPS

## What happens now

1. A 30-minute walkthrough of this report with your team, to answer questions and agree priorities.
2. You can fix everything in-house, use another provider, or ask us for a proposal. The report is yours either way.

Book your own free audit: [tritechsystems.com/free-audit](https://tritechsystems.com/free-audit) | +1 647-277-4813