

## CHG0030114 — [TITAN] High — access\_control on iam-sa-telco-billing-ro

|               |                                   |             |                     |
|---------------|-----------------------------------|-------------|---------------------|
| Severity      | High                              | Priority    | 2 - High            |
| Cloud         | Multi                             | State       | Assigned            |
| Resource      | iam-sa-telco-billing-ro           | Group       | identity_and_access |
| Resource type | iam.googleapis.com/ServiceAccount | Change type | Normal              |
| Opened        | 2026-04-22 18:55:25               | Closed      | 2026-04-22 18:55:25 |
| CAB required  | Yes                               | Close code  | —                   |

### Security Finding

Billing read-only service account was granted roles/owner – drift from intended roles/billing.viewer. Dormant over-privilege and audit-finding exposure.

### Justification

High: Billing read-only service account was granted roles/owner – drift from intended roles/billing.viewer. Dormant over-privilege and audit-finding exposure.

### Implementation Plan

1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:  
`gcloud projects remove-iam-policy-binding <project>  
--member=serviceAccount:iam-sa-telco-billing-ro@<project>.iam.gserviceaccount.com  
--role=roles/owner && gcloud projects add-iam-policy-binding <project>  
--member=serviceAccount:iam-sa-telco-billing-ro@<project>.iam.gserviceaccount.com  
--role=roles/billing.viewer`
3. TITAN FORGE verifies the fix was applied.
4. Post-change rescan by TITAN SCOUT – finding must no longer appear.
5. Close ticket with Successful close\_code.

### Risk & Impact Analysis

Risk level: MEDIUM-HIGH risk – misconfiguration with realistic exploit path.  
Business impact if unremediated: Increases attack surface; auditor finding likely.  
Scope: single resource (iam-sa-telco-billing-ro).  
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available if rescan fails.  
Finding detail: Billing read-only service account was granted roles/owner – drift from intended roles/billing.viewer. Dormant over-privilege and audit-finding exposure.

### Backout / Rollback Plan

1. TITAN auto-captured snapshot of iam-sa-telco-billing-ro before change (baseline: titan-telecom-demo-20260422T201925Z).
2. If post-change rescan still shows the finding OR a new issue appears within 15 min:
  - a. TITAN FORGE fires rollback automatically using stored snapshot.
  - b. Incident reopens and escalates to on-call.
3. Manual rollback command path (human override) is documented in close notes.

### Test Plan

1. TITAN SCOUT rescans iam-sa-telco-billing-ro immediately after FORGE applies the change.
2. PASS criteria: the specific finding no longer appears in SCOUT results.
3. PASS criteria: no new CRITICAL or HIGH findings introduced by the change.
4. Automated compliance check: HIPAA/PCI/SOC2 controls re-evaluated.
5. If any check fails, backout plan fires automatically.

## Recommended Fix Command

```
gcloud projects remove-iam-policy-binding <project>  
--member=serviceAccount:iam-sa-telco-billing-ro@<project>.iam.gserviceaccount.com  
--role=roles/owner && gcloud projects add-iam-policy-binding <project>  
--member=serviceAccount:iam-sa-telco-billing-ro@<project>.iam.gserviceaccount.com  
--role=roles/billing.viewer
```

## Compliance Mapping

CIS 1.x IAM, NIST AC-2, SOC 2 CC6.1, SOC 2 CC7.1

## AI Close Notes

TITAN CONDUIT opened this high access\_control change request and assigned it to the regulatory\_affairs group for review. STATE: ASSIGNED – awaiting human action. Per TITAN AI policy (and Kazmi rule, 2026-04-22), configuration changes are NEVER auto-applied and change tickets are NEVER auto-closed by TITAN. The assigned group reviews the recommended fix, schedules a CAB-approved change window, applies the fix manually, validates via SCOUT rescan, and closes this ticket themselves. TITAN documents and routes – the human owns the change from here.

TITAN AI LLC · CONDUIT Agent · Patent Pending USPTO 19/645,524 · Generated 2026-04-22 20:19 UTC