

CHG0030110 — [TITAN] Medium — logging on sqlsrv-banking-ledger

Severity	Medium	Priority	3 - Moderate
Cloud	Azure	State	Assigned
Resource	sqlsrv-banking-ledger	Group	observability_engineering
Resource type	Microsoft.Sql/servers	Change type	Normal
Opened	2026-04-22 19:19:22	Closed	2026-04-22 19:19:22
CAB required	No	Close code	—

Security Finding

Core-ledger SQL server missing auditing/diagnostic settings – no immutable audit trail for financial transactions. SOX §404 and SOC 1 Type II deficiency.

Justification

Medium: Core-ledger SQL server missing auditing/diagnostic settings – no immutable audit trail for financial transactions. SOX §404 and SOC 1 Type II deficiency.

Implementation Plan

1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
`az sql server audit-policy update --resource-group rg-banking-ledger --name sqlsrv-banking-ledger --state Enabled --storage-account <log-storage> --retention-days 2555`
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 risk – weaker control, should be hardened.
Business impact if unremediated: Control weakness that compounds with other gaps.
Scope: single resource (sqlsrv-banking-ledger).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available if rescan fails.
Finding detail: Core-ledger SQL server missing auditing/diagnostic settings – no immutable audit trail for financial transactions. SOX §404 and SOC 1 Type II deficiency.

Backout / Rollback Plan

1. TITAN auto-captured snapshot of sqlsrv-banking-ledger before change (baseline: titan-banking-demo-20260422T201922Z).
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 sqlsrv-banking-ledger 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

```
az sql server audit-policy update --resource-group rg-banking-ledger --name sqlsrv-banking-ledger  
--state Enabled --storage-account <log-storage> --retention-days 2555
```

Compliance Mapping

SOC 2 CC7.1, HIPAA §164.312(b)

AI Close Notes

TITAN CONDUIT opened this medium logging change request and assigned it to the banking_compliance 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.