INC0010109 — [TITAN] High — kyc on stg-banking-kyc-docs

Severity	High	Priority	2 - High
Cloud	Azure	State	Closed
Resource	stg-banking-kyc-docs	Group	banking_compliance
Resource type	Microsoft.Storage/storageAccounts	Change type	Incident
Opened	2026-04-22 19:25:22	Closed	2026-04-22 19:39:22
CAB required	Yes	Close code	Successful

Security Finding

```
KYC document storage account missing infrastructure-level encryption. FinCEN customer
identification rules and GDPR Art. 32 require encryption at rest for identity documents.
```

Justification

```
High: KYC document storage account missing infrastructure-level encryption. FinCEN customer
identification rules and GDPR Art. 32 require encryption at rest for identity documents.
```

Implementation Plan

```
1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
az storage account update --resource-group rg-banking-kyc --name stgbankingkycdocs
--require-infrastructure-encryption true
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 (stg-banking-kyc-docs).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available
if rescan fails.
Finding detail: KYC document storage account missing infrastructure-level encryption. FinCEN
customer identification rules and GDPR Art. 32 require encryption at rest for identity documents.
```

Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of stg-banking-kyc-docs 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 stg-banking-kyc-docs 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 storage account update --resource-group rg-banking-kyc --name stgbankingkycdocs
--require-infrastructure-encryption true
```

Compliance Mapping

```
HIPAA §164.312(e)(1), PCI DSS 3.4, SOC 2 CC6.1
```

AI Close Notes

```
TITAN CONDUIT orchestrated end-to-end: SCOUT detected the high kyc incident, FORGE applied the
consent-gated fix automatically (incident class), SCOUT rescan confirmed the finding cleared, and
CONDUIT closed this ticket with a Successful close_code. Pre-change snapshot retained for 30 days
for rollback.
```