CHG0030102 — [TITAN] High — encryption on kv-banking-hsm

Severity	High	Priority	2 - High
Cloud	Azure	State	Assigned
Resource	kv-banking-hsm	Group	security_engineering
Resource type	Microsoft.KeyVault/vaults	Change type	Normal
Opened	2026-04-22 20:07:22	Closed	2026-04-22 20:07:22
CAB required	Yes	Close code	—

Security Finding

```
Key Vault 'kv-banking-hsm' soft-delete disabled — HSM-backed keys used for payment processing signing are at risk of irreversible accidental deletion. PCI DSS 3.5.1 requires key management controls.
```

Justification

```
High: Key Vault 'kv-banking-hsm' soft-delete disabled — HSM-backed keys used for payment processing signing are at risk of irreversible accidental deletion. PCI DSS 3.5.1 requires key management controls.
```

Implementation Plan

```
1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
az keyvault update --resource-group rg-banking-core --name kv-banking-hsm --enable-soft-delete true --retention-days 90
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 (kv-banking-hsm).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available if rescan fails.
Finding detail: Key Vault 'kv-banking-hsm' soft-delete disabled — HSM-backed keys used for payment processing signing are at risk of irreversible accidental deletion. PCI DSS 3.5.1 requires key management controls.
```

Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of kv-banking-hsm 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 kv-banking-hsm 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 keyvault update --resource-group rg-banking-core --name kv-banking-hsm --enable-soft-delete true --retention-days 90
```

Compliance Mapping

```
HIPAA §164.312(e)(1), PCI DSS 3.4, SOC 2 CC6.1, PCI DSS 3.5
```

AI Close Notes

```
TITAN CONDUIT opened this high encryption 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.
```