

SIMULATED CASE STUDY

Retest Results

Follow-up of management actions

Engagement	Risk-based ITGC audit (Project 1)
Company	Northstar Financial Technologies (fictional)
Sponsor	Chief Risk Officer (role)
Retest date	2026-09-28
Status as of	2026-09-30

This document is part of a portfolio exercise. Northstar Financial Technologies, its people, systems, records and findings are invented. No real audit was performed, no assurance is given and nothing here is a certification or compliance claim.

1. Purpose

Follow-up of management actions on 2026-09-28. Three actions had a completion date on or before 2026-09-25 and were retested. Observations are simulated: they stand in for the post-remediation evidence an auditor would inspect (system screenshots or exports). One failure was written into the scenario to show how a partial result is reported.

F-01/A1: Terminated employees retained active access to in-scope systems

Action	Disable the 4 remaining active leaver accounts and open a security investigation of the post-termination login	
Retest population	4 accounts that failed the original test	
Evidence inspected	Post-remediation account state as observed on 2026-09-28 (simulated)	
Result	Fail: 1 of 4 records still non-compliant	
Account	Observed state	Result
A-0132	Disabled	Pass
A-0171	Disabled	Pass
A-0218	Disabled	Pass
A-0329	Active	Fail
Unresolved: A-0329 (SYS-04 Developer): still Active, 227 days after the employee's termination on 2026-02-13. The action cannot be closed. The related finding stays open until the account is disabled and the post-termination login investigation is completed.		

F-05/A1: Multi-factor authentication not enabled on some human accounts, including an administrator

Action	Enable MFA on the 3 accounts and disable local authentication for human users	
Retest population	3 accounts that failed the original test	
Evidence inspected	Post-remediation account state as observed on 2026-09-28 (simulated)	
Result	Pass: 3 of 3 records remediated	
Account	Observed state	Result
A-0242	MFA enabled	Pass
A-0390	MFA enabled	Pass
A-0399	MFA enabled	Pass
Nothing unresolved for the records retested. The related finding closes only when every action under it is complete and retested.		

F-06/A1: Dormant and role-change access not removed

Action	Disable the 4 dormant accounts	
Retest population	4 accounts that failed the original test	
Evidence inspected	Post-remediation account state as observed on 2026-09-28 (simulated)	
Result	Pass: 4 of 4 records remediated	
Account	Observed state	Result
A-0232	Disabled	Pass

Account	Observed state	Result
A-0309	Disabled	Pass
A-0315	Disabled	Pass
A-0398	Disabled	Pass
Nothing unresolved for the records retested. The related finding closes only when every action under it is complete and retested.		

Updated finding status as of 2026-09-30

ID	Title	Severity	Status	Retest status
F-01	Terminated employees retained active access to in-scope systems	High	Partially remediated	Retested 2026-09-28: partially remediated
F-02	Administrator access granted without documented approval	High	Remediation in progress	Not yet due
F-03	Quarterly user access reviews were late, incomplete, not independent or ineffective	High	Open	Not yet due
F-04	Service accounts without a valid owner	Medium	Open	Not yet due
F-05	Multi-factor authentication not enabled on some human accounts, including an administrator	High	Closed (retested)	Retested 2026-09-28: remediated
F-06	Dormant and role-change access not removed	Medium	Remediation in progress	Dormant accounts retested 2026-09-28: remediated; mover access not yet due
F-07	Some access was granted before approval, or without an approval record	Low	Risk accepted	Not applicable (risk accepted)
F-08	Developers deployed their own changes to production	High	Open	Not yet due
F-09	Normal changes lacked test evidence, independent approval or prior approval	Medium	Open	Not yet due
F-10	Emergency changes approved retrospectively after the 2-business-day limit	Medium	Open	Not yet due
F-11	Failed backups of the Payments API were not re-run	Medium	Open	Not yet due
F-12	Restoration tests were not evidenced or not successful, and the control has no minimum frequency	Medium	Open	Not yet due
F-13	No restoration test recorded for the Core Ledger or Data Warehouse (inconclusive pending confirmation)	High	Inconclusive: awaiting management confirmation	Not yet due
F-14	Weekly security alert reviews were missing, late, duplicated or lacked escalation	Medium	Open	Not yet due