

SIMULATED CASE STUDY

Final Audit Report

Risk-based IT general controls audit

Engagement	Risk-based ITGC audit (Project 1)
Company	Northstar Financial Technologies (fictional)
Sponsor	Chief Risk Officer (role)
Period	2026-01-01 to 2026-06-30
Report date	2026-09-18
Status	FINAL, simulated

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. Executive summary

The simulated audit tested 15 controls in 16 tests over the period 2026-01-01 to 2026-06-30. It raised 14 findings: 6 High, 7 Medium and 1 Low. One (F-13) is inconclusive: the evidence does not allow a conclusion and it must not be read as a confirmed failure.

The most significant conditions are terminated employees who retained active access (one logged in after termination), administrator access without documented approval, access reviews that did not detect those accounts, developers deploying their own changes to production, and missing or unsuccessful restoration evidence for the payment and ledger systems. This report does not express an opinion on the overall control environment: the testing was scripted over synthetic extracts and did not inspect source documents.

This is the FINAL report. Management responses are included as received on 2026-09-11.

2. Scope, criteria and approach

See the planning memo. In short: five in-scope systems (Customer Portal, Payments API, Core Ledger, Source Control and CI/CD, AWS Production Account), five domains, Northstar's written controls as criteria, and 100% of each extract tested by script. Tolerable deviation is 0% for leaver, privileged, developer-segregation and service-account owner controls and 5% elsewhere. Ratings: High means exposure of Restricted data or payment integrity with a confirmed condition; Medium means a confirmed condition with limited or indirect exposure; Low means isolated exceptions within tolerance and without privileged access.

3. Test results

Test	Control	Population	Exceptions	Conclusion
T-01	NS-IAM-01	408	5	Operating effectively with exceptions (within tolerance)
T-02	NS-IAM-02	35	8	Not operating effectively
T-03	NS-IAM-03	13	2	Not operating effectively
T-04	NS-IAM-04	10	8	Not operating effectively; design deficiency noted
T-05	NS-IAM-05	14	4	Not operating effectively; design deficiency noted
T-06	NS-IAM-06	396	4	Operating effectively with exceptions (within tolerance)
T-07	NS-IAM-07	413	3	Not operating effectively
T-08	NS-PAM-01	19	2	Not operating effectively
T-09	NS-CHG-01	77	5	Not operating effectively
T-10	NS-CHG-02	77	5	Not operating effectively
T-11	NS-CHG-03	91	4	Not operating effectively
T-12	NS-CHG-04	14	3	Not operating effectively
T-13	NS-OPS-01	727	5	Operating effectively with exceptions (within tolerance)
T-14	NS-OPS-02	8	3	Inconclusive; design deficiency noted
T-15	NS-OPS-02	5	2	Not operating effectively
T-16	NS-LOG-02	25	8	Not operating effectively; design deficiency noted

4. Findings summary

ID	Title	Severity	Owner	Target
F-01	Terminated employees retained active access to in-scope systems	High	IT Security Manager	2026-11-17
F-02	Administrator access granted without documented approval	High	Head of Platform Engineering	2026-11-17
F-03	Quarterly user access reviews were late, incomplete, not independent or ineffective	High	IT Security Manager	2026-11-17
F-04	Service accounts without a valid owner	Medium	Head of Platform Engineering	2026-12-17
F-05	Multi-factor authentication not enabled on some human accounts, including an administrator	High	IT Security Manager	2026-11-17
F-06	Dormant and role-change access not removed	Medium	IT Security Manager	2026-12-17
F-07	Some access was granted before approval, or without an approval record	Low	Head of IT Operations	2027-01-16
F-08	Developers deployed their own changes to production	High	Head of Payments Engineering	2026-11-17
F-09	Normal changes lacked test evidence, independent approval or prior approval	Medium	Change Manager	2026-12-17
F-10	Emergency changes approved retrospectively after the 2-business-day limit	Medium	Change Manager	2026-12-17
F-11	Failed backups of the Payments API were not re-run	Medium	Head of IT Operations	2026-12-17
F-12	Restoration tests were not evidenced or not successful, and the control has no minimum frequency	Medium	Head of IT Operations	2026-12-17
F-13	No restoration test recorded for the Core Ledger or Data Warehouse (inconclusive pending confirmation)	High	Head of IT Operations	2026-11-17
F-14	Weekly security alert reviews were missing, late, duplicated or lacked escalation	Medium	IT Security Manager	2026-12-17

5. Detailed findings

F-01: Terminated employees retained active access to in-scope systems [High]

Criteria	NS-IAM-02: access of terminated employees is removed within 2 business days (fictional Access Management Standard).
Condition	8 of 35 leaver accounts (22.9%) were not removed in time. 4 accounts were still Active at the extract date, and 4 were disabled 7 to 15 business days after termination. A-0132 (SYS-02 Payments Console Admin) logged in 6 days after the employee's termination. The HR termination list supplied was partial (EV-002), so further exceptions may exist.
Cause	Offboarding depends on a manual notification from HR to IT; there is no automated deprovisioning from the HR feed, and the quarterly access reviews did not detect the remaining accounts (see F-03). (cause stated by the simulated audit team; not independently verified)
Consequence / risk	A former employee could reach Restricted payment or ledger data. This conflicts with Northstar's low appetite for unauthorised access to Restricted data; confirmed access after termination escalates to the Chief Risk Officer.
Nature of issue	Operating failure
Compensating controls	None relied on. The quarterly access review (NS-IAM-04) is the compensating detective control; it did not operate effectively (F-03), so no reliance is placed on it.
Recommendation	Disable the remaining accounts immediately; investigate the post-termination login to establish who used the account; automate deprovisioning from the HR termination feed and add a daily reconciliation of terminated employees to active accounts.
Evidence	EV-001, EV-002; workpaper(s) WP-T-02
Management response	Agreed: We agree. The four active accounts have been escalated for immediate disablement and a security investigation of the post-termination login has been opened. HR-to-IT automation is planned for the Q4 release.
Accountable role	IT Security Manager
Target date	2026-11-17
Evidence required for closure	All leaver accounts disabled and re-tested on a fresh HR termination list; investigation report on the post-termination login approved by the Chief Risk Officer; evidence of the automated HR-to-IT reconciliation operating for one full month.

F-02: Administrator access granted without documented approval [High]

Criteria	NS-PAM-01: Admin-level access requires system owner approval and documented justification before it is granted.
Condition	2 of 19 Admin accounts (10.5%) have no approval ticket, approver or approval date, on SYS-03, SYS-05.
Cause	Admin access can be granted directly in the administration console without a ticket reference check. (cause stated by the simulated audit team; not independently verified)
Consequence / risk	Unauthorised or excessive privileged access could exist undetected on systems holding Restricted data.
Nature of issue	Operating failure
Compensating controls	None identified in the evidence provided.
Recommendation	Obtain retrospective system-owner approval or remove the access; require a ticket reference before an Admin role can be assigned; add Admin accounts to the monthly privileged access report.
Evidence	EV-001; workpaper(s) WP-T-08
Management response	Agreed. Retrospective approvals will be sought by the target date; accounts without a valid business need will be removed.
Accountable role	Head of Platform Engineering
Target date	2026-11-17
Evidence required for closure	Documented system-owner approval or removal for each Admin account without approval; ticket-reference enforcement shown in configuration evidence; Internal Audit re-performs the Admin population test.

F-03: Quarterly user access reviews were late, incomplete, not independent or ineffective [High]

Criteria	NS-IAM-04: system owners review all accounts each quarter within 30 days of quarter end (design: no independence requirement).
Condition	8 of 10 reviews failed at least one attribute: 1 not completed, 1 completed late, 1 reviewed by a user holding Admin access on the same system, 1 reviewed an incomplete population, and 4 attested as complete although terminated users' accounts remained Active. The control design does not require reviewer independence.
Cause	Reviews are run from spreadsheets without a completeness check, there is no escalation for overdue reviews, and the control text does not prohibit self-review. (cause stated by the simulated audit team; not independently verified)
Consequence / risk	The review is the detective control that should catch inappropriate access (including F-01); when it does not operate, inappropriate access persists.
Nature of issue	Operating failure and design deficiency
Compensating controls	None relied on.
Recommendation	Require reviewer independence in the control text; generate the review population from the system extract and reconcile it before attestation; escalate overdue reviews at day 30; include a leaver check in every review.
Evidence	EV-014, EV-015, EV-016, EV-017, EV-018, EV-019, EV-020, EV-021; workpaper(s) WP-T-04
Management response	Agreed. The control text will be revised for independence and a population reconciliation step added before the Q3 review.
Accountable role	IT Security Manager
Target date	2026-11-17
Evidence required for closure	Revised control text with an independence requirement; the next quarter's review evidenced as complete, on time, independent and reconciled to the system extract, with a leaver check.

F-04: Service accounts without a valid owner [Medium]

Criteria	NS-IAM-05: each service account is assigned an owner when it is created (design: no recertification or reassignment).
Condition	4 of 14 service accounts (28.6%) have no owner (3 with none recorded) or an owner who has left (1 with a terminated owner). The control records an owner only at creation, with no recertification.
Cause	Ownership is not revisited when owners leave; no register reconciliation exists. (cause stated by the simulated audit team; not independently verified)
Consequence / risk	Credentials of unowned service accounts may not be rotated or reviewed, increasing the chance of misuse going unnoticed.
Nature of issue	Design deficiency and operating failure
Compensating controls	None identified.
Recommendation	Assign owners; add owner recertification to the quarterly review; trigger reassignment from the leaver process.
Evidence	EV-001; workpaper(s) WP-T-05
Management response	Agreed.
Accountable role	Head of Platform Engineering
Target date	2026-12-17
Evidence required for closure	Owners assigned to every service account; owner recertification added to the quarterly review; test of the service-account population shows zero accounts without a current owner.

F-05: Multi-factor authentication not enabled on some human accounts, including an administrator [High]

Criteria	NS-IAM-07: MFA is enforced through Corporate SSO for all human accounts on in-scope systems.
Condition	3 of 413 human accounts (0.7%) have MFA disabled, including 1 Admin account.
Cause	These accounts authenticate locally on the system, bypassing Corporate SSO. (cause stated by the simulated audit team; not independently verified)
Consequence / risk	A stolen password alone could give access, including administrator access to source control and CI/CD.
Nature of issue	Operating failure (isolated, but one Admin account)
Compensating controls	Corporate SSO conditional access would compensate for SSO-routed accounts only; it does not cover these local accounts.
Recommendation	Enable MFA on the three accounts; disable local authentication for human users; alert on accounts outside SSO.
Evidence	EV-001; workpaper(s) WP-T-07
Management response	Agreed. MFA enabled; local authentication to be disabled by the target date.
Accountable role	IT Security Manager
Target date	2026-11-17
Evidence required for closure	MFA flag verified enabled on the three accounts in the live console; local authentication for human users disabled (configuration evidence).

F-06: Dormant and role-change access not removed [Medium]

Criteria	NS-IAM-06: accounts idle over 90 days are disabled unless excepted. NS-IAM-03: access follows role changes within 30 days.
Condition	4 human accounts of current employees were idle more than 90 days without an exception, and 2 movers kept access from their previous department more than 30 days after transfer.
Cause	The monthly dormant-account list is produced but not consistently actioned; movers are not part of the leaver trigger. (cause stated by the simulated audit team; not independently verified)
Consequence / risk	Unused access widens the attack surface; retained role access breaks least-privilege and segregation expectations.
Nature of issue	Operating failure
Compensating controls	Monthly dormant-account list exists but was not actioned; treated as not compensating.
Recommendation	Disable dormant accounts automatically after 90 days with a manager exception route; add a mover review to the transfer workflow.
Evidence	EV-001; workpaper(s) WP-T-06, WP-T-03
Management response	Agreed with modification: We agree on the facts but rate the dormant-account condition Low, because the idle accounts hold Standard privilege. Internal Audit retains the Medium rating because one mover retains access to the Payments API and the dormant-account process failed repeatedly.
Accountable role	IT Security Manager
Target date	2026-12-17
Evidence required for closure	Dormant accounts disabled and a re-run of the idle-account test shows no unexcepted accounts over 90 days; mover access removed and a mover review step evidenced for the next two transfers.

F-07: Some access was granted before approval, or without an approval record [Low]

Criteria	NS-IAM-01: access is provisioned only after documented approval by the requester's line manager.
Condition	5 of 408 non-Admin accounts (1.2%) have no approval record (2) or an approval dated after the grant (3). Admin accounts are tested separately in T-08 and reported in F-02.
Cause	Approval is attached to the request ticket after provisioning in some cases; no automated check blocks provisioning without a ticket. (cause stated by the simulated audit team; not independently verified)
Consequence / risk	Access might not have been authorised when it was granted. Exception rate is within the 5% tolerance and none involves Admin access.
Nature of issue	Isolated exceptions
Compensating controls	Monthly ticket-existence report proposed by management as the mitigating control; not yet operating, so no reliance.
Recommendation	Require a ticket reference at provisioning; report accounts without a ticket monthly.
Evidence	EV-001; workpaper(s) WP-T-01
Management response	Risk accepted: Residual risk is below the executive threshold and is accepted by the risk owner with the monthly ticket report as a mitigating control.
Accountable role	Head of IT Operations
Target date	2027-01-16
Evidence required for closure	Not applicable (risk accepted). Accepted by the risk owner; revisit if the exception rate exceeds tolerance at the next audit.

F-08: Developers deployed their own changes to production [High]

Criteria	NS-CHG-03: the deployer of a Normal or Emergency change is not its developer.
Condition	4 of 91 Normal and Emergency changes (4.4%) were deployed by their own developer, on SYS-01, SYS-02, SYS-03, SYS-05, including payment and ledger systems.
Cause	Deployment permissions in the pipeline are not separated from developer roles for some engineers. (cause stated by the simulated audit team; not independently verified)
Consequence / risk	Unreviewed code could reach production without a second person, enabling error or fraud in payment systems.
Nature of issue	Operating failure
Compensating controls	Peer review of code (NS-SDL-01) would compensate if it operated; it was not tested in this engagement, so no reliance is placed on it.
Recommendation	Technically enforce separation of developer and deployer roles in the pipeline; review pipeline permissions quarterly.
Evidence	EV-003; workpaper(s) WP-T-11
Management response	Agreed. Pipeline role separation will be enforced; interim monitoring is in place.
Accountable role	Head of Payments Engineering
Target date	2026-11-17
Evidence required for closure	Pipeline configuration shows developer and deployer roles are separated; a re-run of the deployer-versus-developer test over the next quarter has zero exceptions.

F-09: Normal changes lacked test evidence, independent approval or prior approval [Medium]

Criteria	NS-CHG-01 and NS-CHG-02: independent approval before implementation; recorded Pass test result.
Condition	Of 77 Normal changes, 5 had no recorded test result, 2 were approved by their requester and 3 were approved after implementation.
Cause	The change tool allows closing a change without mandatory test and approval fields. (cause stated by the simulated audit team; not independently verified)
Consequence / risk	Defective or unauthorised changes might reach production, including the Payments API and Core Ledger.
Nature of issue	Operating failure
Compensating controls	None identified.
Recommendation	Make test result, evidence reference and independent approver mandatory fields; block implementation without prior approval.
Evidence	EV-003; workpaper(s) WP-T-09, WP-T-10
Management response	Agreed. Field validation is in the tool backlog.
Accountable role	Change Manager
Target date	2026-12-17
Evidence required for closure	Mandatory test, evidence and independent approver fields live in the change tool; a re-test over the next quarter's Normal changes has zero exceptions.

F-10: Emergency changes approved retrospectively after the 2-business-day limit [Medium]

Criteria	NS-CHG-04: retrospective approval within 2 business days.
Condition	3 of 14 Emergency changes (21.4%) were approved 6 to 15 business days after implementation. All are on SYS-01.
Cause	No reminder or escalation is triggered when retrospective approval is outstanding. (cause stated by the simulated audit team; not independently verified)
Consequence / risk	Emergency changes remain unreviewed for weeks.
Nature of issue	Operating failure
Compensating controls	None identified.
Recommendation	Automate reminders at day 1 and escalation at day 2.
Evidence	EV-003; workpaper(s) WP-T-12
Management response	Agreed.
Accountable role	Change Manager
Target date	2026-12-17
Evidence required for closure	Automated day-1 reminder and day-2 escalation in operation; next quarter's Emergency changes all approved within 2 business days.

F-11: Failed backups of the Payments API were not re-run [Medium]

Criteria	NS-OPS-01: failed jobs are re-run and any failure not resolved within 24 hours is escalated.
Condition	5 failed backup jobs on SYS-02 (dates: 2026-02-03, 2026-03-17, 2026-05-11, 2026-05-12, 2026-05-13) have no successful re-run. No escalation records were provided.
Cause	The on-duty engineer is notified but there is no ticket or tracking for failed jobs. (cause stated by the simulated audit team; not independently verified)
Consequence / risk	Recovery points for the Payments API are missing for the affected dates, increasing potential data loss.
Nature of issue	Operating failure
Compensating controls	None identified in the evidence provided.
Recommendation	Create an automatic ticket for each failed backup with an escalation timer; report unresolved failures weekly.
Evidence	EV-004; workpaper(s) WP-T-13
Management response	Agreed.
Accountable role	Head of IT Operations
Target date	2026-12-17
Evidence required for closure	Failed-job tickets with escalation timers in operation; a re-test of the next quarter shows every failure retried or escalated within 24 hours.

F-12: Restoration tests were not evidenced or not successful, and the control has no minimum frequency [Medium]

Criteria	NS-OPS-02 (design) against the backup standard, which requires quarterly restoration testing.
Condition	Of 5 recorded restoration tests, 1 had no evidence and 1 ended Partial. The control states testing occurs 'as scheduling permits', which has no minimum frequency and is weaker than the quarterly requirement of the backup standard.
Cause	The control was written before the backup standard was updated. (cause stated by the simulated audit team; not independently verified)
Consequence / risk	Backups could be unrecoverable and the first discovery would be during a real incident.
Nature of issue	Design deficiency and operating failure (evidence)
Compensating controls	None identified.
Recommendation	Align the control with a quarterly minimum; require evidence retention; investigate and re-run the Partial test.
Evidence	EV-005, EV-022, EV-023, EV-024, EV-025; workpaper(s) WP-T-15, WP-T-14
Management response	Agreed. The control text will be aligned to the quarterly requirement.
Accountable role	Head of IT Operations
Target date	2026-12-17
Evidence required for closure	Control text aligned to quarterly testing; evidence retained for every test; the Partial restoration test re-run with a Pass result.

F-13: No restoration test recorded for the Core Ledger or Data Warehouse (inconclusive pending confirmation) [High]

Criteria	NS-OPS-02 and the backup standard: quarterly restoration testing of critical systems.
Condition	No restoration test is recorded for SYS-03 Core Ledger in 2026-Q1 or 2026-Q2, or for SYS-07 Data Warehouse in 2026-Q2. The restore register is maintained manually and its owner has not confirmed that it is complete (EV-005), so the absence of tests is not confirmed. Daily backups of the Core Ledger ran during the period.
Cause	Not determined: either tests were not run, or they were run and not recorded. (cause stated by the simulated audit team; not independently verified)
Consequence / risk	If tests were not run, the Core Ledger (Restricted data; low appetite for outages) could be unrecoverable.
Nature of issue	Evidence insufficiency (not a confirmed control failure)
Compensating controls	Daily backups ran for the Core Ledger during the period; backups alone do not demonstrate recoverability.
Recommendation	Owner to confirm completeness of the register and provide evidence of any tests; if none were run, perform a ledger restoration test within 30 days. Internal Audit will reassess on receipt.
Evidence	EV-005; workpaper(s) WP-T-14
Management response	Agreed: The register owner is reviewing records; a ledger restoration test is scheduled for October regardless.
Accountable role	Head of IT Operations
Target date	2026-11-17
Evidence required for closure	The register owner confirms completeness in writing, or a ledger restoration test is performed and evidenced. Internal Audit then updates the conclusion to confirmed or cleared.

F-14: Weekly security alert reviews were missing, late, duplicated or lacked escalation [Medium]

Criteria	NS-LOG-02: weekly review within 5 business days of week end; high-severity alerts escalated (design: escalation is discretionary).
Condition	Of 25 weeks, 3 had no review, 2 were reviewed late, 2 had high-severity alerts with none escalated, and 1 record duplicated another. The control leaves escalation to analyst discretion. The recorded hash of the evidence file does not match its current hash (EV-006).
Cause	Review coverage depends on individual analysts; the SIEM does not enforce a weekly review task or a mandatory escalation decision. (cause stated by the simulated audit team; not independently verified)
Consequence / risk	High-severity alerts may not be actioned, and monitoring gaps can delay detection of incidents.
Nature of issue	Operating failure and design deficiency
Compensating controls	None identified.
Recommendation	Make escalation of high alerts mandatory with a documented decision; schedule review tasks with tracking; control the review log so it cannot be edited after the fact.
Evidence	EV-006; workpaper(s) WP-T-16
Management response	Agreed.
Accountable role	IT Security Manager
Target date	2026-12-17
Evidence required for closure	Control text requires an escalation decision for every high alert; four consecutive months of complete, timely reviews on a tamper-evident log.

6. Observations on evidence reliability

These concern the evidence supplied by management, not control failures. They reduce reliance on the affected evidence and are reported so that they are not mistaken for independent corroboration.

Rule	Evidence	Observation
R-EVD-01	EV-007	EV-007 (identity_access_extract_2026-07-15 (1).csv): Re-sent by the owner after a follow-up request.
R-EVD-01	EV-008	EV-008 (change_export_H1_2026_full.csv): Provided in response to a question about June changes.
R-EVD-02	EV-003	EV-003 (change_export_H1_2026.csv): Export parameters show an end date of 2026-05-31.
R-EVD-02	EV-004	EV-004 (backup_job_log_2026-02-01_to_2026-06-30.csv): Export parameters show a start date of 2026-02-01.
R-EVD-03	EV-006	EV-006 (weekly_alert_review_log.csv): Log extract re-saved by the owner after collection.
R-EVD-04	EV-002	EV-002 (hr_terminations_2026-02-01_to_2026-06-30.csv): HR states the list excludes terminations before 2026-02-01.
R-EVD-04	EV-005	EV-005 (restore_test_register.csv): Register maintained manually; completeness not confirmed by owner.

7. Limitations

Synthetic data; scripted tests over one extract date; no inspection of source tickets; causes are the simulated audit team's explanation; ratings are the audit team's judgement; eighteen library controls were not tested (reasons in the audit program); the results cannot be generalised to any real organisation.

8. Management action plan (summary)

Action	Finding	Owner	Target	Status at issue
F-01/A1	F-01	IT Security Manager	2026-09-25	Planned
F-01/A2	F-01	IT Security Manager	2026-11-17	Planned
F-02/A1	F-02	Head of Platform Engineering	2026-11-17	Not started
F-03/A1	F-03	IT Security Manager	2026-11-17	Not started
F-04/A1	F-04	Head of Platform Engineering	2026-12-17	Not started
F-05/A1	F-05	IT Security Manager	2026-09-25	Planned
F-06/A1	F-06	IT Security Manager	2026-09-25	Planned
F-06/A2	F-06	IT Security Manager	2026-12-17	Planned
F-07/A1	F-07	Head of IT Operations	2027-01-16	Not started
F-08/A1	F-08	Head of Payments Engineering	2026-11-17	Not started
F-09/A1	F-09	Change Manager	2026-12-17	Not started
F-10/A1	F-10	Change Manager	2026-12-17	Not started
F-11/A1	F-11	Head of IT Operations	2026-12-17	Not started
F-12/A1	F-12	Head of IT Operations	2026-12-17	Not started
F-13/A1	F-13	Head of IT Operations	2026-11-17	Not started
F-14/A1	F-14	IT Security Manager	2026-12-17	Not started

Statuses after the 2026-09-28 retest are in the retest results report.