

SIMULATED CASE STUDY

Audit Planning Memo

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
Status	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. Purpose and sponsor

This memo records the planning decisions for a simulated risk-based IT general controls (ITGC) audit of Northstar Financial Technologies, a fictional Canadian business-payments company. The engagement sponsor is the Chief Risk Officer (a role, not a person). The exercise demonstrates audit planning, scripted control testing, evidence handling, reporting and retesting using synthetic data.

2. Audit objective

To assess whether selected ITGCs over identity and access, privileged access, change management, IT operations (backup and restoration) and logging and monitoring operated as designed for the period 2026-01-01 to 2026-06-30, and to report weaknesses with evidence, root cause and recommendations. The report does not express an assurance opinion.

3. Scope and exclusions

Systems in scope	SYS-01 Customer Portal, SYS-02 Payments API, SYS-03 Core Ledger, SYS-04 Source Control and CI/CD, SYS-05 AWS Production Account
Audit period	2026-01-01 to 2026-06-30
Fieldwork	2026-07-13 to 2026-08-28
Population extract date	2026-07-15
Domains	Identity and access; privileged access; change management; IT operations (backup and restoration); logging and monitoring
Controls tested	15 of 33 controls in the library (15 tested, 18 not tested; reasons in the audit program)
Exclusions	Other systems, physical security, application business logic, privacy, vendor risk (Project 3), AI governance (Project 4), incident response, vulnerability management and secure development

4. Criteria

Northstar's own written control statements (the control library, NS-xxx-nn) and its fictional policy set: Access Control Policy v3.2, Change Management Policy v2.4, Backup and Recovery Standard v2.0, Logging and Monitoring Standard v1.7 and Information Security Policy v4.0 (evidence items EV-009 to EV-013). Policy thresholds are held in one reference file: 2 business days to remove leaver access, 90 days dormancy, access reviews due 30 days after quarter end, emergency changes approved within 2 business days, weekly alert reviews within 5 business days, backup retries within 24 hours and quarterly restoration tests. Mappings to external frameworks are handled in Project 2 and are not used as audit criteria here.

5. Independence statement

The fictional audit team reports to the Audit Committee, not to the owners of the systems audited, and has no operational responsibility for them. In this simulation the work was prepared with AI assistance; no human independence review took place.

6. Approach

Risk-based: the five risks with the highest inherent scores that map to ITGC domains were selected (below). Populations are system extracts taken on 2026-07-15. Because each extract is complete, the full population is tested by script rather than a sample, which removes sampling error and makes every result re-performable. This is not a statistical method and no statistical assurance is claimed. Source tickets and screenshots behind each record were not inspected. A result is Pass within the tolerable deviation (0% for leaver, privileged, developer-segregation and service-account owner controls, 5% for the rest), Fail above it, and Inconclusive where evidence is incomplete or unreliable. Design deficiencies are reported separately from operating failures, and compensating controls are credited only where they were themselves tested.

7. Preliminary risk assessment

Risk	Title	Inherent	Priority	Mgmt residual	Selected	Domain / reason
R-01	Inappropriate or unremoved user access	20	High	12	Yes	Identity and access (IAM)
R-02	Misuse of privileged access	15	High	8	Yes	Privileged access (PAM)
R-03	Unauthorised or untested production change	16	High	9	Yes	Change management (CHG)
R-04	Data loss or unrecoverable systems	15	High	12	Yes	IT operations: backup and restoration (OPS)
R-05	Security events not detected or acted on	12	Medium	6	Yes	Logging and monitoring (LOG)
R-06	Critical vendor failure	15	High	8	No	Outside ITGC domains selected, or covered by Project 3/4 (see audit program)
R-07	Vendor data exposure	12	Medium	9	No	Outside ITGC domains selected, or covered by Project 3/4 (see audit program)
R-08	Incorrect AI-generated customer response	12	Medium	9	No	Outside ITGC domains selected, or covered by Project 3/4 (see audit program)
R-09	Sensitive data exposed through an AI tool	15	High	12	No	Outside ITGC domains selected, or covered by Project 3/4 (see audit program)
R-10	Payment card data compromise	10	Medium	8	No	Outside ITGC domains selected, or covered by Project 3/4 (see audit program)
R-11	Unremediated vulnerabilities	16	High	9	No	Outside ITGC domains selected, or covered by Project 3/4 (see audit program)
R-12	Privacy breach or non-compliant retention	12	Medium	6	No	Outside ITGC domains selected, or covered by Project 3/4 (see audit program)
R-13	Insecure software development	12	Medium	6	No	Outside ITGC domains selected, or covered by Project 3/4 (see audit program)
R-14	Delayed incident response and notification	12	Medium	6	No	Outside ITGC domains selected, or covered by Project 3/4 (see audit program)

Scores are Northstar's own pre-audit assessments from the risk register (likelihood x impact on a 5 x 5 scale). Management residual scores are management's view before this audit and are not validated by it.

8. Audit universe

System	Name	Criticality	Classification	Card scope	In scope	Rationale
SYS-01	Customer Portal	Critical	Confidential	Connected	Y	Critical or Restricted-data production system supporting payments; in scope.
SYS-02	Payments API	Critical	Restricted	In scope	Y	Critical or Restricted-data production system supporting payments; in scope.
SYS-03	Core Ledger	Critical	Restricted	Out of scope	Y	Critical or Restricted-data production system supporting payments; in scope.
SYS-04	Source Control and CI/CD	High	Confidential	Connected	Y	In scope (shared platform for in-scope systems).
SYS-05	AWS Production Account	Critical	Restricted	In scope	Y	Critical or Restricted-data production system supporting payments; in scope.
SYS-06	Corporate SSO	Critical	Confidential	Connected	N	Out of scope: lower inherent risk for this engagement or covered by another project; may be audited in a later cycle.
SYS-07	Data Warehouse	High	Confidential	Out of scope	N	Out of scope: lower inherent risk for this engagement or covered by another project; may be audited in a later cycle.
SYS-08	Security Monitoring (SIEM)	High	Confidential	Connected	N	Out of scope: lower inherent risk for this engagement or covered by another project; may be audited in a later cycle.
SYS-09	Support Ticketing	Medium	Confidential	Out of scope	N	Out of scope: lower inherent risk for this engagement or covered by another project; may be audited in a later cycle.
SYS-10	HR Information System	Medium	Confidential	Out of scope	N	Out of scope: lower inherent risk for this engagement or covered by another project; may be audited in a later cycle.
SYS-11	Knowledge Base	Medium	Internal	Out of scope	N	Out of scope: lower inherent risk for this engagement or covered by another project; may be audited in a later cycle.
SYS-12	Document Repository	Medium	Confidential	Out of scope	N	Out of scope: lower inherent risk for this engagement or covered by another project; may be audited in a later cycle.
SYS-13	Vendor Management Register	Low	Internal	Out of scope	N	Out of scope: lower inherent risk for this engagement or covered by another project; may be audited in a later cycle.
SYS-14	Backup and Recovery Service	High	Confidential	Connected	N	Out of scope: lower inherent risk for this engagement or covered by another project; may be audited in a later cycle.

9. Risk-based scope rationale

Access (R-01) and privileged access (R-02) carry the highest inherent scores because they protect Restricted payment and ledger data, which Northstar has a low appetite to expose. Change management (R-03) is next because the Payments API and Core Ledger change frequently. Backup and restoration (R-04) is included because the ledger is the system of record. Logging and monitoring (R-05) is the detective layer over all of them. Vendor, privacy, AI and secure-development risks are real but are covered by other projects or by later cycles, and are recorded as not tested rather than ignored.

10. Timeline

Milestone	Date
Evidence requested	2026-07-06
Population extract	2026-07-15
Fieldwork	2026-07-13 to 2026-08-28
Draft report to management	2026-09-04
Management responses due	2026-09-11
Final report	2026-09-18
Follow-up retest	2026-09-28
Status as of	2026-09-30

11. Evidence requests

31 evidence items were requested and received (see evidence-request-list.csv). Evidence reliability problems found during fieldwork are reported in the final report: duplicate files, a period that does not match the data, a file whose hash changed after collection, and two incomplete populations.

12. Limitations

Synthetic data; one population extract date; full-population scripted testing without inspection of source documents; control design assessed from written text only; no interviews actually held; the entitlement map and policy thresholds are fictional; the results say nothing about any real organisation.

Appendix A. Walkthrough and interview questions

Identity and access (joiners, movers, leavers)

- How is a joiner's access requested, approved and provisioned? Who can provision without a ticket?
- How does the HR termination event reach IT? Is it automated or manual, and who checks that every leaver account was disabled?
- How are role changes (movers) detected and who removes access that belonged to the previous role?
- How is the quarterly access review population produced, who reviews it, and how is its completeness checked?
- Who owns service accounts and what happens when an owner leaves?

Privileged access

- Who can grant Admin access, and what evidence of approval and business justification is retained?
- How is break-glass administrator access issued, time-limited and reviewed?

Change management

- Which change types exist and what approval, testing and deployment roles apply to each?
- Can a change be closed without a test result or approver? Who can deploy to production?
- How are emergency changes approved after the fact and what reminds approvers?

IT operations

- How are failed backups detected, re-run and escalated? Who is on duty?
- How often are restores tested, who decides, and where is the register kept? Who confirms it is complete?

Logging and monitoring

- Who reviews SIEM alerts each week, and what happens to high-severity alerts?
- Can review records be edited after completion?