

SIMULATED CASE STUDY

Executive Risk and Assurance Dashboard Summary

Northstar Financial Technologies, cross-project view

Version	1.0
As-of date	2026-09-30
Source	data/processed/dashboard.json
Generated by	scripts/build_dashboard_reports.py

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. Summary

As of 2026-09-30, the fictional Northstar programme has 12 open audit findings (5 High, 7 Medium), 6 overdue remediation items, 2 of 3 assessed vendors at High residual risk, and no AI use case approved without conditions. All figures are computed from the shared synthetic datasets by scripts/build_dashboard_data.py and reconcile to the downloadable CSV files.

A management-reported completion that failed the audit retest is counted as not complete. Enterprise risk residual scores are the pre-audit values and have not been re-rated; the audit findings are shown beside them as a signal for the risk owners.

2. Key indicators

ID	Indicator	Value	Source
K01	Open audit findings	12 findings	data/analysis/findings.csv
K02H	Open High findings	5 findings	data/analysis/findings.csv
K02M	Open Medium findings	7 findings	data/analysis/findings.csv
K02L	Open Low findings	0 findings	data/analysis/findings.csv
K03	Overdue remediation items	6 items	data/analysis/remediation_actions.csv
K04	Controls tested not operating effectively	12 tests	data/analysis/control_tests.csv
K05	Vendors with High residual risk	2 vendors	projects/03-third-party-risk/vendor-risk-register.csv
K06	AI use cases approved to proceed (unconditionally)	0 use cases	projects/04-ai-governance/ai-use-case-inventory.csv
K07	AI approval gates evidenced	0 of 16 gates	projects/04-ai-governance/ai-approval-gates.csv
K08	Audit-readiness gaps identified	54 gaps	projects/02-unified-controls/audit-readiness-gap-assessment.csv
K09	Actionable gaps (excluding Not applicable)	50 gaps	projects/02-unified-controls/audit-readiness-gap-assessment.csv
K10	AI evidence review: exception recall (held-out, assisted mode)	0.93 ratio	projects/05-ai-evidence-review/evaluation.json
K11	Enterprise risks needing executive acceptance (recorded residual >= 15)	0 risks	data/raw-synthetic/risks.csv

3. Charts as tables

C1. Findings by severity and status

Project 1 findings by severity, split into open and closed/accepted.

Severity	Open	Closed or accepted	Total
High	5	1	6
Medium	7	0	7
Low	0	1	1

C2. Open findings by time to target date

Open findings grouped by days from the as-of date to the target remediation date. All findings share one final-report date (2026-09-18), so finding age is the same for each; time to target date is shown instead.

Time to target date	High	Medium	Low
Due within 30 days	0	0	0
Due in 31-60 days	5	0	0
Due in 61-90 days	0	7	0
Due in more than 90 days	0	0	0

C3. Open findings by control domain

Domain taken from the control cited in each finding's criteria reference.

Domain	High	Medium	Low	Total
Change management	1	2	0	3
IT operations	1	2	0	3
Identity and access	2	2	0	4
Logging and monitoring	0	1	0	1
Privileged access	1	0	0	1

C4. Control test outcomes

Project 1 test conclusions. No test concluded fully effective with zero exceptions. 4 tests also noted a design deficiency.

Outcome	Tests
Effective with exceptions within tolerance	3
Not operating effectively	12
Inconclusive	1

C5. Project 1 remediation actions by validated state

Management-reported status combined with the audit retest result. 'Reported complete, retest failed' is not counted as done.

State	Actions
Not started	11
In progress	2
Complete and retest passed	2
Reported complete, retest failed	1

C6. Open vendor issues by age and severity

Open or in-progress Project 3 vendor issues; age = as-of date minus opened date.

Age since opened	High	Medium	Low
0-14 days	11	2	0
15-30 days	0	0	0
31+ days	2	1	2

C7. Vendor inherent vs residual risk

Residual risk applies the documented step rule to the evidence status. Only 3 vendors were assessed. Vendor V-02 moves up because of unanswered questionnaire items.

Vendor	Tier	Inherent	Residual	Movement
Stratwick Managed Hosting Inc.	Tier 1	High	High	Same
Pinebrook Print and Mail Ltd.	Tier 3	Low	Medium	Up

Vendor	Tier	Inherent	Residual	Movement
Lumenvale AI Ltd.	Tier 2	Medium	High	Up

C8. AI use-case decisions and risk

Committee decision, risk ratings and gate progress for the two proposed AI use cases.

Use case	Name	Decision	Inherent	Residual as proposed	Target after gates	Gates evidenced
AI-01	Customer Support Response Assistant	Conditionally approved (limited pilot)	High	High	Medium	0 of 8
AI-02	Policy and Procedure Document Analyser	Not approved: must not proceed	High	High	Medium	0 of 8

C11. Audit-readiness gaps by type and roadmap phase

Phase = the 30/60/90-day roadmap slot each gap is scheduled in.

Gap type	By day 30	By day 60	By day 90	Total
Design weakness	3	2	2	7
Mapping uncertainty	0	3	6	9
Missing control	1	1	3	5
Missing evidence	1	5	12	18
Not applicable	0	0	4	4
Operating failure	5	5	1	11

C12. AI evidence review variants (held-out 108 cases)

Held-out evaluation of three review variants. Mock model, author-labelled synthetic cases, no human review. Recall confidence intervals for rules-only and assisted overlap.

Variant	Precision	Recall	F1	False-positive rate	Abstention rate
Rules only	0.94	0.7	0.8	0.057	0.33
Mock text-only	0.95	0.95	0.95	0.057	0.08
Assisted	0.95	0.93	0.94	0.057	0.19

C10. Enterprise risks and open audit findings

Open findings linked to each risk through the control cited.

Risk	Title	Recorded residual	Open P1 findings	High
R-01	Inappropriate or unremoved user access	12	4	2
R-02	Misuse of privileged access	8	1	1
R-03	Unauthorised or untested production change	9	3	1
R-04	Data loss or unrecoverable systems	12	3	1
R-05	Security events not detected or acted on	6	1	0
R-06	Critical vendor failure	8	0	0
R-07	Vendor data exposure	9	0	0
R-08	Incorrect AI-generated customer response	9	0	0
R-09	Sensitive data exposed through an AI tool	12	0	0
R-10	Payment card data compromise	8	0	0

Risk	Title	Recorded residual	Open P1 findings	High
R-11	Unremediated vulnerabilities	9	0	0
R-12	Privacy breach or non-compliant retention	6	0	0
R-13	Insecure software development	6	0	0
R-14	Delayed incident response and notification	6	0	0

4. Method and limitations

Definitions, formulas, inclusion rules and source files for every indicator are in the indicator sheet of the workbook and in docs/dashboard-methodology.md. Counts depend on small synthetic populations, so percentages move a lot with a single record. The audit-test selection was risk-based, not random, so test outcomes do not describe the whole control environment. The AI evidence-review indicator comes from a prototype using a mock model and author-labelled cases; it is illustrative only.