

SIMULATED CASE STUDY

30-60-90 Day Remediation Roadmap

Unified control framework

Project	Unified control framework and audit readiness (Project 2)
Company	Northstar Financial Technologies (fictional)
Status	Simulated; mappings are draft author judgement
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

Remediation roadmap ordered by priority and dependency. Every item has an accountable role, acceptance criteria and the evidence needed to close it. Effort is an estimate for planning only.

2. Roadmap

By day 30

Item	Control	Action	Owner	Depends on	Acceptance	Evidence to close
RM-001	UC-ACC-02	Remediate the operating failure and retest the same population (Control did not operate effectively in Project 1: T-02 8 of 35 leaver accounts failed (22.9%). Findings F-01.).	IT Security Manager		Retest of the same population shows no exceptions beyond tolerance.	Retest workpaper and the post-remediation extract with hash.
RM-002	UC-ACC-03	Remediate the operating failure and retest the same population (Control did not operate effectively in Project 1: T-04 8 of 10 quarterly reviews failed (80.0%). Findings F-03.).	IT Security Manager		Retest of the same population shows no exceptions beyond tolerance.	Retest workpaper and the post-remediation extract with hash.
RM-003	UC-ACC-07	Remediate the operating failure and retest the same population (Control did not operate effectively in Project 1: T-07 3 of 413 human accounts failed (0.7%). Findings F-05.).	IT Security Manager		Retest of the same population shows no exceptions beyond tolerance.	Retest workpaper and the post-remediation extract with hash.
RM-004	UC-ACC-02	Revise the control design: Policy allows 2 business days; the PCI DSS wording (8.2.5) says terminated users' access is revoked immediately. For the Payments API segment the policy is weaker than the requirement as worded. Confirm interpretation with an assessor before changing policy.	IT Security Manager		Revised control text approved by the control owner and Chief Risk Officer; next test uses the new criteria.	Approved control text with version and approval record.
RM-005	UC-ACC-03	Revise the control design: Control does not require reviewer independence (P1 T-04). Quarterly frequency is stricter than the six-month PCI DSS cadence (7.2.4) but must also cover third-party accounts.	IT Security Manager		Revised control text approved by the control owner and Chief Risk Officer; next test uses the new criteria.	Approved control text with version and approval record.
RM-006	UC-ACC-01	Remediate the operating failure and retest the same population (Control did not operate effectively in Project 1: T-03 2 of 13 mover accounts failed (15.4%). Findings F-06, F-07.).	IT Service Desk Manager		Retest of the same population shows no exceptions beyond tolerance.	Retest workpaper and the post-remediation extract with hash.
RM-007	UC-ACC-05	Remediate the operating failure and retest the same population (Control did not operate effectively in Project 1: T-05 4 of 14 service accounts failed (28.6%). Findings F-04.).	Head of Platform Engineering		Retest of the same population shows no exceptions beyond tolerance.	Retest workpaper and the post-remediation extract with hash.
RM-008	UC-GOV-02	Design, approve and start operating the control. No asset or data inventory control exists in the Northstar library; scoping and vulnerability coverage depend on it.	Head of IT Operations		Control documented with owner, frequency and evidence; first operation evidenced.	Control document and first-cycle evidence.
RM-009	UC-ACC-05	Revise the control design: Owner recorded at creation only; no recertification or reassignment on owner departure (P1 T-05).	Head of Platform Engineering		Revised control text approved by the control owner and Chief Risk Officer; next test uses the new criteria.	Approved control text with version and approval record.

Item	Control	Action	Owner	Depends on	Acceptance	Evidence to close
RM-010	UC-ACC-02	Obtain or confirm the evidence: Evidence EV-002 is unreliable or incomplete: HR termination list is partial (excludes terminations before 2026-02-01).	IT Security Manager		Evidence is complete for the period, reliable (hash recorded and matching) and accepted by the tester.	Provider confirmation, re-extract with hash, updated evidence register.

By day 60

Item	Control	Action	Owner	Depends on	Acceptance	Evidence to close
RM-011	UC-CHG-02	Remediate the operating failure and retest the same population (Control did not operate effectively in Project 1: T-11 4 of 91 Normal and Emergency changes failed (4.4%). Findings F-08.).	Head of Payments Engineering		Retest of the same population shows no exceptions beyond tolerance.	Retest workpaper and the post-remediation extract with hash.
RM-012	UC-ACC-04	Remediate the operating failure and retest the same population (Control did not operate effectively in Project 1: T-08 2 of 19 admin accounts failed (10.5%). Findings F-02.).	Head of Platform Engineering		Retest of the same population shows no exceptions beyond tolerance.	Retest workpaper and the post-remediation extract with hash.
RM-013	UC-BCR-02	Remediate the operating failure and retest the same population (Control did not operate effectively in Project 1: T-15 2 of 5 restoration tests failed (40.0%). Findings F-12, F-13.).	Head of IT Operations		Retest of the same population shows no exceptions beyond tolerance.	Retest workpaper and the post-remediation extract with hash.
RM-014	UC-CHG-01	Revise the control design: No requirement for a security-impact assessment or a procedure to return to a secure state after a failed change, both of which PCI DSS 6.5.1 lists.	Change Manager		Revised control text approved by the control owner and Chief Risk Officer; next test uses the new criteria.	Approved control text with version and approval record.
RM-015	UC-CHG-01	Remediate the operating failure and retest the same population (Control did not operate effectively in Project 1: T-09 5 of 77 Normal changes failed (6.5%); T-10 5 of 77 Normal changes failed (6.5%). Findings F-09.).	Change Manager		Retest of the same population shows no exceptions beyond tolerance.	Retest workpaper and the post-remediation extract with hash.
RM-016	UC-CHG-03	Remediate the operating failure and retest the same population (Control did not operate effectively in Project 1: T-12 3 of 14 Emergency changes failed (21.4%). Findings F-10.).	Change Manager		Retest of the same population shows no exceptions beyond tolerance.	Retest workpaper and the post-remediation extract with hash.
RM-017	UC-BCR-02	Obtain or confirm the evidence: Project 1 could not conclude: restore register completeness not confirmed (EV-005); absence of tests is not confirmed. Finding F-12, F-13 is inconclusive.	Head of IT Operations		Evidence is complete for the period, reliable (hash recorded and matching) and accepted by the tester.	Provider confirmation, re-extract with hash, updated evidence register.
RM-018	UC-CFG-01	Design, approve and start operating the control. No secure configuration baseline control exists in the Northstar library.	Head of Platform Engineering	UC-GOV-02	Control documented with owner, frequency and evidence; first operation evidenced.	Control document and first-cycle evidence.
RM-019	UC-VUL-01	Obtain or confirm the evidence: No operating evidence was obtained for NS-VUL-01 in Project 1 (not tested).	Head of Platform Engineering	UC-GOV-02	Evidence is complete for the period, reliable (hash recorded and matching) and accepted by the tester.	Provider confirmation, re-extract with hash, updated evidence register.
RM-020	UC-VUL-01	Resolve the open mapping question: Northstar's control covers critical vulnerabilities within 30 days only; PCI DSS 6.3.3 requires critical or high within one month. Treated as a possible gap pending confirmation of how Northstar ranks vulnerabilities.	Head of Platform Engineering	UC-GOV-02	Mapping reviewed by a second person and, where relevant, an assessor; confidence and review status updated.	Review record and updated crosswalk row.

Item	Control	Action	Owner	Depends on	Acceptance	Evidence to close
RM-021	UC-CHG-01	Obtain or confirm the evidence: Evidence EV-003 is unreliable or incomplete: Stated evidence period ends 2026-05-31 but the data contains June changes.	Change Manager		Evidence is complete for the period, reliable (hash recorded and matching) and accepted by the tester.	Provider confirmation, re-extract with hash, updated evidence register.
RM-022	UC-SUP-01	Obtain or confirm the evidence: No operating evidence was obtained for NS-SUP-01 in Project 1 (not tested).	Head of Procurement		Evidence is complete for the period, reliable (hash recorded and matching) and accepted by the tester.	Provider confirmation, re-extract with hash, updated evidence register.
RM-023	UC-AIG-01	Obtain or confirm the evidence: No operating evidence was obtained for NS-AIG-01 in Project 1 (not tested). Project 4 proposes the policy, intake, approval gates and monitoring for this area; none of it is operating yet, so it is not operating evidence.	AI Governance Committee		Evidence is complete for the period, reliable (hash recorded and matching) and accepted by the tester.	Provider confirmation, re-extract with hash, updated evidence register.
RM-024	UC-BCR-02	Revise the control design: Control says testing occurs 'as scheduling permits', with no minimum frequency, against a quarterly backup standard (P1 T-14).	Head of IT Operations		Revised control text approved by the control owner and Chief Risk Officer; next test uses the new criteria.	Approved control text with version and approval record.
RM-025	UC-BCR-02	Resolve the open mapping question: No requirement for restoration testing was identified in the PCI DSS requirements verified (offline media storage, 9.4.1.1, is a different topic). Backups of the Payments API segment may hold account data, so applicability needs an assessor's view.	Head of IT Operations		Mapping reviewed by a second person and, where relevant, an assessor; confidence and review status updated.	Review record and updated crosswalk row.
RM-026	UC-SUP-01	Resolve the open mapping question: PCI DSS 12.8 applies only to providers that handle or can affect account data. Whether Stratwick Managed Hosting (V-01) falls in scope is an open question for Project 3.	Head of Procurement		Mapping reviewed by a second person and, where relevant, an assessor; confidence and review status updated.	Review record and updated crosswalk row.

By day 90

Item	Control	Action	Owner	Depends on	Acceptance	Evidence to close
RM-027	UC-BCR-03	Obtain or confirm the evidence: No operating evidence was obtained for NS-OPS-03 in Project 1 (not tested).	Head of IT Operations	UC-BCR-02	Evidence is complete for the period, reliable (hash recorded and matching) and accepted by the tester.	Provider confirmation, re-extract with hash, updated evidence register.
RM-028	UC-BCR-03	Resolve the open mapping question: No PCI DSS requirement for disaster recovery testing was identified in the verified subset; incident-plan content (12.10.1) lists business recovery and continuity procedures but is a different control.	Head of IT Operations	UC-BCR-02	Mapping reviewed by a second person and, where relevant, an assessor; confidence and review status updated.	Review record and updated crosswalk row.
RM-029	UC-LOG-02	Revise the control design: Escalation of high alerts is discretionary (P1 T-16), and weekly review is slower than the daily review in PCI DSS 10.4.1 for the Payments API segment.	IT Security Manager		Revised control text approved by the control owner and Chief Risk Officer; next test uses the new criteria.	Approved control text with version and approval record.
RM-030	UC-LOG-01	Revise the control design: Retention is 12 months but the control does not state that three months must be immediately available for analysis (PCI DSS 10.5.1).	IT Security Manager	UC-GOV-02	Revised control text approved by the control owner and Chief Risk Officer; next test uses the new criteria.	Approved control text with version and approval record.
RM-031	UC-LOG-02	Remediate the operating failure and retest the same population (Control did not operate effectively in Project 1: T-16 8 of 25 weeks failed (32.0%). Findings F-14.).	IT Security Manager		Retest of the same population shows no exceptions beyond tolerance.	Retest workpaper and the post-remediation extract with hash.
RM-032	UC-GOV-01	Design, approve and start operating the control. No policy-governance control exists in the Northstar library although the policy set is cited as criteria.	Chief Risk Officer		Control documented with owner, frequency and evidence; first operation evidenced.	Control document and first-cycle evidence.
RM-033	UC-GOV-03	Design, approve and start operating the control. No security awareness training control exists in the Northstar library.	Head of People		Control documented with owner, frequency and evidence; first operation evidenced.	Control document and first-cycle evidence.
RM-034	UC-AIG-01	Resolve the open mapping question: None of the four selected frameworks addresses AI governance in specific terms. NIST AI RMF and ISO/IEC 42001 are handled in Project 4; mappings here are Low confidence.	AI Governance Committee		Mapping reviewed by a second person and, where relevant, an assessor; confidence and review status updated.	Review record and updated crosswalk row.
RM-035	UC-AIG-01	Record the applicability decision: PCI DSS mapping not made: the control is outside the assumed Payments API segment scope (scope assumption, not a compliance conclusion).	AI Governance Committee		Decision documented and approved by the Chief Risk Officer.	Signed applicability statement.
RM-036	UC-LOG-01	Obtain or confirm the evidence: No operating evidence was obtained for NS-LOG-01, NS-LOG-03 in Project 1 (not tested).	IT Security Manager	UC-GOV-02	Evidence is complete for the period, reliable (hash recorded and matching) and accepted by the tester.	Provider confirmation, re-extract with hash, updated evidence register.

Item	Control	Action	Owner	Depends on	Acceptance	Evidence to close
RM-037	UC-INC-01	Obtain or confirm the evidence: No operating evidence was obtained for NS-INC-01 in Project 1 (not tested).	IT Security Manager		Evidence is complete for the period, reliable (hash recorded and matching) and accepted by the tester.	Provider confirmation, re-extract with hash, updated evidence register.
RM-038	UC-INC-02	Obtain or confirm the evidence: No operating evidence was obtained for NS-INC-02 in Project 1 (not tested).	IT Security Manager		Evidence is complete for the period, reliable (hash recorded and matching) and accepted by the tester.	Provider confirmation, re-extract with hash, updated evidence register.
RM-039	UC-SUP-02	Obtain or confirm the evidence: No operating evidence was obtained for NS-SUP-02 in Project 1 (not tested).	Head of Procurement		Evidence is complete for the period, reliable (hash recorded and matching) and accepted by the tester.	Provider confirmation, re-extract with hash, updated evidence register.
RM-040	UC-PRV-01	Obtain or confirm the evidence: No operating evidence was obtained for NS-PRV-01 in Project 1 (not tested).	Privacy Officer		Evidence is complete for the period, reliable (hash recorded and matching) and accepted by the tester.	Provider confirmation, re-extract with hash, updated evidence register.
RM-041	UC-PRV-02	Obtain or confirm the evidence: No operating evidence was obtained for NS-PRV-02 in Project 1 (not tested).	Privacy Officer		Evidence is complete for the period, reliable (hash recorded and matching) and accepted by the tester.	Provider confirmation, re-extract with hash, updated evidence register.
RM-042	UC-SDL-01	Obtain or confirm the evidence: No operating evidence was obtained for NS-SDL-01, NS-SDL-02 in Project 1 (not tested).	VP Engineering		Evidence is complete for the period, reliable (hash recorded and matching) and accepted by the tester.	Provider confirmation, re-extract with hash, updated evidence register.
RM-043	UC-AIG-02	Obtain or confirm the evidence: No operating evidence was obtained for NS-AIG-02 in Project 1 (not tested). Project 4 proposes the policy, intake, approval gates and monitoring for this area; none of it is operating yet, so it is not operating evidence.	Head of Customer Support		Evidence is complete for the period, reliable (hash recorded and matching) and accepted by the tester.	Provider confirmation, re-extract with hash, updated evidence register.
RM-044	UC-AIG-03	Obtain or confirm the evidence: No operating evidence was obtained for NS-AIG-03 in Project 1 (not tested). Project 4 proposes the policy, intake, approval gates and monitoring for this area; none of it is operating yet, so it is not operating evidence.	AI Governance Committee		Evidence is complete for the period, reliable (hash recorded and matching) and accepted by the tester.	Provider confirmation, re-extract with hash, updated evidence register.
RM-045	UC-SUP-02	Resolve the open mapping question: As UC-SUP-01: applicability of PCI DSS 12.8.4 and 12.8.5 depends on which vendors affect the payments environment.	Head of Procurement		Mapping reviewed by a second person and, where relevant, an assessor; confidence and review status updated.	Review record and updated crosswalk row.

Item	Control	Action	Owner	Depends on	Acceptance	Evidence to close
RM-046	UC-LOG-02	Obtain or confirm the evidence: Evidence EV-006 is unreliable or incomplete: Recorded hash of the alert review log does not match the file.	IT Security Manager		Evidence is complete for the period, reliable (hash recorded and matching) and accepted by the tester.	Provider confirmation, re-extract with hash, updated evidence register.
RM-047	UC-GOV-04	Design, approve and start operating the control. No control confirms the card-data scope annually; the scope in the scenario document is an assumption.	Head of Payments Engineering	UC-GOV-02	Control documented with owner, frequency and evidence; first operation evidenced.	Control document and first-cycle evidence.
RM-048	UC-VUL-02	Obtain or confirm the evidence: No operating evidence was obtained for NS-VUL-02 in Project 1 (not tested).	Head of Payments Engineering		Evidence is complete for the period, reliable (hash recorded and matching) and accepted by the tester.	Provider confirmation, re-extract with hash, updated evidence register.
RM-049	UC-AIG-02	Resolve the open mapping question: No verified outcome concerns human review of AI output; mapping is Low confidence.	Head of Customer Support		Mapping reviewed by a second person and, where relevant, an assessor; confidence and review status updated.	Review record and updated crosswalk row.
RM-050	UC-AIG-03	Resolve the open mapping question: No verified outcome concerns AI monitoring; mapping is Low confidence.	AI Governance Committee		Mapping reviewed by a second person and, where relevant, an assessor; confidence and review status updated.	Review record and updated crosswalk row.
RM-051	UC-PRV-01	Resolve the open mapping question: Canadian and Ontario privacy obligations were not researched beyond the PIPEDA principles; applicability to Northstar is assumed, not concluded.	Privacy Officer		Mapping reviewed by a second person and, where relevant, an assessor; confidence and review status updated.	Review record and updated crosswalk row.
RM-052	UC-PRV-01	Record the applicability decision: PCI DSS mapping not made: the control is outside the assumed Payments API segment scope (scope assumption, not a compliance conclusion).	Privacy Officer		Decision documented and approved by the Chief Risk Officer.	Signed applicability statement.
RM-053	UC-AIG-02	Record the applicability decision: PCI DSS mapping not made: the control is outside the assumed Payments API segment scope (scope assumption, not a compliance conclusion).	Head of Customer Support		Decision documented and approved by the Chief Risk Officer.	Signed applicability statement.
RM-054	UC-AIG-03	Record the applicability decision: PCI DSS mapping not made: the control is outside the assumed Payments API segment scope (scope assumption, not a compliance conclusion).	AI Governance Committee		Decision documented and approved by the Chief Risk Officer.	Signed applicability statement.