

SIMULATED CASE STUDY

Audit Readiness Gap Assessment

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. Summary

The unified library holds 32 controls: 27 consolidated from the 33 Northstar controls and 5 proposed because the crosswalk showed topics with no Northstar control. There are 158 mapping rows to NIST CSF 2.0, ISO/IEC 27001:2022 Annex A, PCI DSS (Payments API segment only), SOC 2 categories and PIPEDA principles. The assessment found 54 gaps: 11 operating failure, 7 design weakness, 5 missing control, 18 missing evidence, 9 mapping uncertainty, 4 not applicable.

A mapping is a judgement that two statements overlap. It is not evidence of compliance, and nothing here claims ISO/IEC 27001 certification, SOC 2 attestation or PCI DSS compliance.

2. How to read it

Gap types: operating failure (the control ran and failed its test), design weakness (the written control is weaker than the policy or the framework wording), missing control (nothing in the library covers the topic), missing evidence (not tested, or evidence incomplete or unreliable), mapping uncertainty (the mapping cannot be made with confidence) and not applicable (scope decision). Priority score = inherent risk score (1-25) + 3 for operating failure or missing control, +2 for design weakness or missing evidence, +2 if the gap involves a High finding, +2 if it involves a PCI DSS requirement for the Payments API segment. Phase: score 22 or more by day 30, 17 or more by day 60, otherwise day 90; an item that depends on another is placed at least 30 days after it. Effort (S days, M weeks, L months) is the author's planning estimate, not a measurement.

3. Gaps by phase

Phase	Gaps
By day 30	10
By day 60	16
By day 90	28

4. Gap register

ID	Control	Type	Description	Score	Effort	Phase
GAP-002	UC-ACC-02	Operating failure	Control did not operate effectively in Project 1: T-02 8 of 35 leaver accounts failed (22.9%). Findings F-01.	25	M	30
GAP-003	UC-ACC-03	Operating failure	Control did not operate effectively in Project 1: T-04 8 of 10 quarterly reviews failed (80.0%). Findings F-03.	25	M	30
GAP-006	UC-ACC-07	Operating failure	Control did not operate effectively in Project 1: T-07 3 of 413 human accounts failed (0.7%). Findings F-05.	25	M	30
GAP-032	UC-ACC-02	Design weakness	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.	24	M	30
GAP-033	UC-ACC-03	Design weakness	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.	24	S	30
GAP-001	UC-ACC-01	Operating failure	Control did not operate effectively in Project 1: T-03 2 of 13 mover accounts failed (15.4%). Findings F-06, F-07.	23	M	30
GAP-005	UC-ACC-05	Operating failure	Control did not operate effectively in Project 1: T-05 4 of 14 service accounts failed (28.6%). Findings F-04.	23	M	30
GAP-028	UC-GOV-02	Missing control	No asset or data inventory control exists in the Northstar library; scoping and vulnerability coverage depend on it.	23	L	30
GAP-034	UC-ACC-05	Design weakness	Owner recorded at creation only; no recertification or reassignment on owner departure (P1 T-05).	22	S	30
GAP-048	UC-ACC-02	Missing evidence	Evidence EV-002 is unreliable or incomplete: HR termination list is partial (excludes terminations before 2026-02-01).	22	M	30
GAP-008	UC-CHG-02	Operating failure	Control did not operate effectively in Project 1: T-11 4 of 91 Normal and Emergency changes failed (4.4%). Findings F-08.	21	M	60
GAP-004	UC-ACC-04	Operating failure	Control did not operate effectively in Project 1: T-08 2 of 19 admin accounts failed (10.5%). Findings F-02.	20	M	60
GAP-016	UC-BCR-02	Operating failure	Control did not operate effectively in Project 1: T-15 2 of 5 restoration tests failed (40.0%). Findings F-12, F-13.	20	M	60
GAP-039	UC-CHG-01	Design weakness	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.	20	S	60
GAP-007	UC-CHG-01	Operating failure	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.	19	M	60
GAP-009	UC-CHG-03	Operating failure	Control did not operate effectively in Project 1: T-12 3 of 14 Emergency changes failed (21.4%). Findings F-10.	19	M	60
GAP-017	UC-BCR-02	Missing 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.	19	S	60
GAP-030	UC-CFG-01	Missing control	No secure configuration baseline control exists in the Northstar library.	19	L	60
GAP-010	UC-VUL-01	Missing evidence	No operating evidence was obtained for NS-VUL-01 in Project 1 (not tested).	18	S	60
GAP-047	UC-VUL-01	Mapping uncertainty	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.	18	S	60
GAP-050	UC-CHG-01	Missing evidence	Evidence EV-003 is unreliable or incomplete: Stated evidence period ends 2026-05-31 but the data contains June changes.	18	S	60

ID	Control	Type	Description	Score	Effort	Phase
GAP-019	UC-SUP-01	Missing evidence	No operating evidence was obtained for NS-SUP-01 in Project 1 (not tested).	17	S	60
GAP-024	UC-AIG-01	Missing 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.	17	S	60
GAP-035	UC-BCR-02	Design weakness	Control says testing occurs 'as scheduling permits', with no minimum frequency, against a quarterly backup standard (P1 T-14).	17	S	60
GAP-036	UC-BCR-02	Mapping uncertainty	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.	17	S	60
GAP-044	UC-SUP-01	Mapping uncertainty	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.	17	S	60
GAP-018	UC-BCR-03	Missing evidence	No operating evidence was obtained for NS-OPS-03 in Project 1 (not tested).	17	S	90
GAP-037	UC-BCR-03	Mapping uncertainty	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.	17	S	90
GAP-038	UC-LOG-02	Design weakness	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.	16	S	90
GAP-040	UC-LOG-01	Design weakness	Retention is 12 months but the control does not state that three months must be immediately available for analysis (PCI DSS 10.5.1).	16	S	90
GAP-013	UC-LOG-02	Operating failure	Control did not operate effectively in Project 1: T-16 8 of 25 weeks failed (32.0%). Findings F-14.	15	M	90
GAP-027	UC-GOV-01	Missing control	No policy-governance control exists in the Northstar library although the policy set is cited as criteria.	15	M	90
GAP-029	UC-GOV-03	Missing control	No security awareness training control exists in the Northstar library.	15	M	90
GAP-041	UC-AIG-01	Mapping uncertainty	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.	15	S	90
GAP-052	UC-AIG-01	Not applicable	PCI DSS mapping not made: the control is outside the assumed Payments API segment scope (scope assumption, not a compliance conclusion).	15	S	90
GAP-012	UC-LOG-01	Missing evidence	No operating evidence was obtained for NS-LOG-01, NS-LOG-03 in Project 1 (not tested).	14	S	90
GAP-014	UC-INC-01	Missing evidence	No operating evidence was obtained for NS-INC-01 in Project 1 (not tested).	14	S	90
GAP-015	UC-INC-02	Missing evidence	No operating evidence was obtained for NS-INC-02 in Project 1 (not tested).	14	S	90
GAP-020	UC-SUP-02	Missing evidence	No operating evidence was obtained for NS-SUP-02 in Project 1 (not tested).	14	S	90
GAP-021	UC-PRV-01	Missing evidence	No operating evidence was obtained for NS-PRV-01 in Project 1 (not tested).	14	S	90
GAP-022	UC-PRV-02	Missing evidence	No operating evidence was obtained for NS-PRV-02 in Project 1 (not tested).	14	S	90

ID	Control	Type	Description	Score	Effort	Phase
GAP-023	UC-SDL-01	Missing evidence	No operating evidence was obtained for NS-SDL-01, NS-SDL-02 in Project 1 (not tested).	14	S	90
GAP-025	UC-AIG-02	Missing 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.	14	S	90
GAP-026	UC-AIG-03	Missing 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.	14	S	90
GAP-045	UC-SUP-02	Mapping uncertainty	As UC-SUP-01: applicability of PCI DSS 12.8.4 and 12.8.5 depends on which vendors affect the payments environment.	14	S	90
GAP-049	UC-LOG-02	Missing evidence	Evidence EV-006 is unreliable or incomplete: Recorded hash of the alert review log does not match the file.	14	S	90
GAP-031	UC-GOV-04	Missing control	No control confirms the card-data scope annually; the scope in the scenario document is an assumption.	13	S	90
GAP-011	UC-VUL-02	Missing evidence	No operating evidence was obtained for NS-VUL-02 in Project 1 (not tested).	12	S	90
GAP-042	UC-AIG-02	Mapping uncertainty	No verified outcome concerns human review of AI output; mapping is Low confidence.	12	S	90
GAP-043	UC-AIG-03	Mapping uncertainty	No verified outcome concerns AI monitoring; mapping is Low confidence.	12	S	90
GAP-046	UC-PRV-01	Mapping uncertainty	Canadian and Ontario privacy obligations were not researched beyond the PIPEDA principles; applicability to Northstar is assumed, not concluded.	12	S	90
GAP-051	UC-PRV-01	Not applicable	PCI DSS mapping not made: the control is outside the assumed Payments API segment scope (scope assumption, not a compliance conclusion).	12	S	90
GAP-053	UC-AIG-02	Not applicable	PCI DSS mapping not made: the control is outside the assumed Payments API segment scope (scope assumption, not a compliance conclusion).	12	S	90
GAP-054	UC-AIG-03	Not applicable	PCI DSS mapping not made: the control is outside the assumed Payments API segment scope (scope assumption, not a compliance conclusion).	12	S	90

5. Limits of this assessment

Crosswalk rows cover only the references listed in the source register as verified or partially verified. ISO Annex A titles come from a secondary source and PCI DSS wording was read from the v4.0 document, not v4.0.1. SOC 2 is mapped at category level because the criteria text could not be accessed. Unmapped requirements are not gaps; they were not assessed. Operating status comes from Project 1's scripted tests over synthetic data and says nothing about any real organisation.