

SIMULATED CASE STUDY

Vendor Assessment Pack: Pinebrook Print and Mail Ltd.

Third-party risk assessment

Project	Third-party risk and remediation (Project 3)
Company	Northstar Financial Technologies (fictional)
Vendors	Fictional; none represents a real company
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. Vendor and service

Vendor	Pinebrook Print and Mail Ltd. (V-02)
Service	Printing and mailing of customer statements
Criticality / data	Low / Confidential
Contract	2023-09-01 to 2026-12-31
Owner	Head of Operations
Tier	Tier 3 (weighted total 11)
Inherent risk	Low
Residual risk (at committee date 2026-09-17)	Medium: 3 of 4 required evidence areas are not verified: Retention and deletion (Unclear term); Subcontractors and subprocessors (Not provided); Access control (Self-reported)
Target residual if conditions met	Low (assumption)
Decision	Conditionally approve

2. Evidence by area

Area	Required	Status	Gap?
Independent assurance report	No	Not provided	No
Access control	Yes	Self-reported	Yes
Encryption	No	Self-reported	No
Retention and deletion	Yes	Unclear term	Yes
Subcontractors and subprocessors	Yes	Not provided	Yes
Incident notification	Yes	Contractual (clear)	No
Business continuity and recovery	No	Not provided	No
Penetration testing	No	Not provided	No
Model training and data use	No	Not applicable	No

3. Evidence register

ID	Area	Evidence	Reliance	Period	Gap or exception
VE-010	Independent assurance report	ISO/IEC 27001 certificate (claimed in questionnaire)	None	n/a	Vendor states it holds an ISO/IEC 27001 certificate but supplied no certificate, scope statement or certification body name. Claim not verified.
VE-011	Access control	Security questionnaire response: access control section	Self-reported	n/a	None noted
VE-012	Encryption	Security questionnaire response: file transfer encryption	Self-reported	n/a	None noted
VE-013	Retention and deletion	Data processing agreement: retention of statement files	Contractual	2023-09-01 to 2026-12-31	Agreement says files are deleted 'after completion of the service' with no number of days and no deletion confirmation.
VE-014	Subcontractors and subprocessors	Security questionnaire response: subcontractors	None	n/a	Question left unanswered. Pinebrook uses a courier, so a subcontractor exists but is not identified.
VE-015	Incident notification	Data processing agreement: incident notification clause	Contractual	2023-09-01 to 2026-12-31	None noted
VE-016	Business continuity and recovery	Security questionnaire response: continuity	None	n/a	Section unanswered (questionnaire 18 of 40 questions answered).
A gap listed above means the control could not be assessed from the evidence provided, or the evidence has a stated limitation. It is not by itself proof that the vendor's control failed.					

4. Decision

Conditionally approve. Continue statement printing; review at contract end 2026-12-31.

Rationale: Low criticality and a manual fallback mean the evidence gaps do not justify stopping the service, but the vendor holds customers' names and addresses and has not evidenced its claims.

Conditions

1. Complete the 22 unanswered security questions
2. Provide the ISO/IEC 27001 certificate and scope statement, or withdraw the claim
3. Name the courier subcontractor and confirm its handling of statements
4. Amend the agreement to state a deletion deadline and require deletion confirmation

Escalation triggers: Conditions not met by 2026-12-01 (30 days before the contract ends) or any loss or misdelivery of statements.

Accountable owner: Head of Operations. Residual risk acceptance authority: Risk owner (business owner role).

5. Issues

Issue	Area	Severity	Owner	Due	Status	Overdue days
TPR-007	Independent assurance report	Low	Pinebrook Print and Mail Ltd. (via Head of Operations)	2026-09-07	Open	23
TPR-008	Retention and deletion	Medium	Pinebrook Print and Mail Ltd. (via Head of Operations)	2026-12-01	Open	0
TPR-009	Subcontractors and subprocessors	Medium	Pinebrook Print and Mail Ltd. (via Head of Operations)	2026-09-07	Open	23
TPR-010	Business continuity and recovery	Low	Pinebrook Print and Mail Ltd. (via Head of Operations)	2026-09-07	Closed	0
TPR-011	Access control	Medium	Pinebrook Print and Mail Ltd. (via Head of Operations)	2026-12-01	Open	0

6. What would change the assessment

Independent evidence for the unverified areas and signed clarification of unclear terms would remove the gaps; the target assumes all conditions are met and validated.