

SIMULATED CASE STUDY

Vendor Decision Memo

Comparative committee memo

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
Committee date	2026-09-17

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. Decision requested

The committee is asked to approve the decisions below for three vendors assessed between 2026-08-17 and 2026-09-17. Residual risk acceptance for Stratwick and Lumenvale rests with the Chief Risk Officer because residual risk is High.

Vendor	Tier	Inherent	Residual	Decision	Acceptance authority
V-01 Stratwick Managed Hosting Inc.	Tier 1	High	High	Conditionally approve	Chief Risk Officer (executive acceptance)
V-02 Pinebrook Print and Mail Ltd.	Tier 3	Low	Medium	Conditionally approve	Risk owner (business owner role)
V-03 Lumenvale AI Ltd.	Tier 2	Medium	High	Restrict	Chief Risk Officer (executive acceptance)

V-01 Stratwick Managed Hosting Inc.: Conditionally approve

Continue the managed hosting service.

The service is critical and hard to replace, so rejecting is not realistic in the short term. Residual risk is currently High because the evidence has a six-month gap, an access exception and an unassessed DR site, so the Chief Risk Officer must accept it for a limited period while conditions are met.

Conditions

- Obtain a bridge letter or equivalent covering 2026-04-01 to 2026-09-30 by 2026-11-01 (condition precedent to the 2027-03-31 renewal discussion)
- Obtain evidence that the user-access-removal exception was fixed and validated by the service auditor or by Northstar re-performance
- Obtain independent assurance, or a plan to obtain it, over the disaster recovery site
- Close Northstar's own leaver-removal and MFA findings (F-01, F-05), because they are the CUECs Northstar must operate
- Obtain penetration test retest evidence for the two medium findings

Escalation triggers: Bridge letter not received by 2026-11-01, a qualified opinion, or a confirmed security incident at Stratwick.

V-02 Pinebrook Print and Mail Ltd.: Conditionally approve

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

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

- Complete the 22 unanswered security questions
- Provide the ISO/IEC 27001 certificate and scope statement, or withdraw the claim
- Name the courier subcontractor and confirm its handling of statements
- 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.

V-03 Lumenvale AI Ltd.: Restrict

Permitted only for AI-01 under the Project 4 gates, using content approved for the API tier. Not permitted for the document-upload tier or for AI-02 until terms are clarified.

Retention, training use, subprocessors and incident terms are all unclear, so residual risk is High. Rejecting would end an approved pilot unnecessarily, so use is restricted to the narrowest case until the terms are clear.

Conditions

- Written confirmation of prompt and output retention, and a signed zero-retention or equivalent option
- Written confirmation that customer content in every tier, including document upload, is not used for model training
- Subprocessor list with hosting regions and a change-notice commitment
- Incident notification clause with a stated time limit, content and a named contact
- Privacy review of cross-border handling of personal information
- A SOC 2 Type II report or independent penetration test summary

Escalation triggers: Any unanswered condition after 2026-11-01, a vendor change to retention or training terms, or a vendor incident.

Open issues at 2026-09-30

Issue	Vendor	Area	Severity	Due	Status	Overdue	Escalation
TPR-001	V-01	Independent assurance report	High	2026-11-01	Open	0	None
TPR-002	V-01	Access control	High	2026-11-01	In progress	0	None
TPR-003	V-01	Access control	High	2026-11-01	In progress	0	None
TPR-004	V-01	Subcontractors and subprocessors	High	2026-11-01	Open	0	None
TPR-005	V-01	Business continuity and recovery	High	2026-11-01	Open	0	None
TPR-007	V-02	Independent assurance report	Low	2026-09-07	Open	23	Head of Procurement
TPR-008	V-02	Retention and deletion	Medium	2026-12-01	Open	0	None
TPR-009	V-02	Subcontractors and subprocessors	Medium	2026-09-07	Open	23	Head of Procurement
TPR-011	V-02	Access control	Medium	2026-12-01	Open	0	None
TPR-012	V-03	Independent assurance report	High	2026-11-01	Open	0	None
TPR-013	V-03	Retention and deletion	High	2026-11-01	Open	0	None
TPR-014	V-03	Subcontractors and subprocessors	High	2026-09-07	Open	23	Head of Procurement
TPR-015	V-03	Incident notification	High	2026-11-01	Open	0	None
TPR-016	V-03	Business continuity and recovery	High	2026-09-07	Open	23	Head of Procurement
TPR-017	V-03	Penetration testing	Low	2026-09-07	Open	23	Head of Procurement
TPR-018	V-03	Model training and data use	High	2026-11-01	Open	0	None
TPR-019	V-03	Access control	High	2026-11-01	Open	0	None
TPR-020	V-03	Encryption	High	2026-11-01	Open	0	None

Assumptions and limits

Vendors and their evidence are fictional. Decisions follow the documented method; the scoring is ordinal judgement. Not-provided evidence is a gap, not a failure. Closure of an issue needs validation by Northstar.