

SIMULATED CASE STUDY

Vendor Assessment Pack: Lumenvale AI 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	Lumenvale AI Ltd. (V-03)
Service	Hosted large-language-model API used for text drafting and summarisation
Criticality / data	Medium / Confidential
Contract	2026-08-01 to 2027-07-31
Owner	Chief Product Officer
Tier	Tier 2 (weighted total 16)
Inherent risk	Medium
Residual risk (at committee date 2026-09-17)	High: 8 of 8 required evidence areas are not verified: Independent assurance report (Verified with exception or limitation); Access control (Self-reported); Encryption (Self-reported); Retention and deletion (Unclear term); Subcontractors and subprocessors (Not provided); Incident notification (Unclear term); Business continuity and recovery (Not provided); Model training and data use (Unclear term)
Target residual if conditions met	Medium (assumption)
Decision	Restrict

2. Evidence by area

Area	Required	Status	Gap?
Independent assurance report	Yes	Verified with exception or limitation	Yes
Access control	Yes	Self-reported	Yes
Encryption	Yes	Self-reported	Yes
Retention and deletion	Yes	Unclear term	Yes
Subcontractors and subprocessors	Yes	Not provided	Yes
Incident notification	Yes	Unclear term	Yes
Business continuity and recovery	Yes	Not provided	Yes
Penetration testing	No	Not provided	No
Model training and data use	Yes	Unclear term	Yes

3. Evidence register

ID	Area	Evidence	Reliance	Period	Gap or exception
VE-017	Independent assurance report	SOC 2 Type I report	Independent	2026-03-31 to 2026-03-31	Type I describes design at a single date; it does not test operating effectiveness over a period.
VE-018	Access control	Security questionnaire response: access control	Self-reported	n/a	None noted
VE-019	Encryption	Security questionnaire response: encryption	Self-reported	n/a	None noted
VE-020	Retention and deletion	Terms of service and data processing addendum: prompt and output retention	Contractual	2026-08-01 to 2027-07-31	Terms say prompts may be retained 'for up to 30 days for abuse monitoring' on the standard tier; a zero-retention option exists but is not part of the signed order, and it is unclear which tier the document-upload feature uses.
VE-021	Subcontractors and subprocessors	Subprocessor list	None	n/a	List 'available on request' was requested on 2026-08-17 and not provided. Hosting region is assumed to be the United States.
VE-022	Incident notification	Data processing addendum: incident notification clause	Contractual	2026-08-01 to 2027-07-31	Clause says 'without undue delay' with no time limit, no content requirements and no named contact.
VE-023	Business continuity and recovery	Security questionnaire response: continuity	None	n/a	Not answered.
VE-024	Penetration testing	Penetration test summary	None	n/a	Requested; vendor says a summary is available under NDA only. Not provided.
VE-025	Model training and data use	Terms of service: use of customer content for model training	Contractual	2026-08-01 to 2027-07-31	Terms say customer data from the API is not used for training, but are silent on the document-upload tier. Cannot confirm the position for AI-02.
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

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.

Rationale: 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

1. Written confirmation of prompt and output retention, and a signed zero-retention or equivalent option
2. Written confirmation that customer content in every tier, including document upload, is not used for model training
3. Subprocessor list with hosting regions and a change-notice commitment
4. Incident notification clause with a stated time limit, content and a named contact
5. Privacy review of cross-border handling of personal information
6. 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.

Accountable owner: Chief Product Officer. Residual risk acceptance authority: Chief Risk Officer (executive acceptance).

5. Issues

Issue	Area	Severity	Owner	Due	Status	Overdue days
TPR-012	Independent assurance report	High	Lumenvale AI Ltd. (via Chief Product Officer)	2026-11-01	Open	0
TPR-013	Retention and deletion	High	Lumenvale AI Ltd. (via Chief Product Officer)	2026-11-01	Open	0
TPR-014	Subcontractors and subprocessors	High	Lumenvale AI Ltd. (via Chief Product Officer)	2026-09-07	Open	23
TPR-015	Incident notification	High	Lumenvale AI Ltd. (via Chief Product Officer)	2026-11-01	Open	0
TPR-016	Business continuity and recovery	High	Lumenvale AI Ltd. (via Chief Product Officer)	2026-09-07	Open	23
TPR-017	Penetration testing	Low	Lumenvale AI Ltd. (via Chief Product Officer)	2026-09-07	Open	23
TPR-018	Model training and data use	High	Lumenvale AI Ltd. (via Chief Product Officer)	2026-11-01	Open	0
TPR-019	Access control	High	Lumenvale AI Ltd. (via Chief Product Officer)	2026-11-01	Open	0
TPR-020	Encryption	High	Lumenvale AI Ltd. (via Chief Product Officer)	2026-11-01	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.