

SIMULATED CASE STUDY

Vendor Assessment Pack: Stratwick Managed Hosting Inc.

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	Stratwick Managed Hosting Inc. (V-01)
Service	Managed database hosting and disaster-recovery site for the payments environment
Criticality / data	Critical / Restricted
Contract	2022-04-01 to 2027-03-31
Owner	Head of Payments Engineering
Tier	Tier 1 (weighted total 26)
Inherent risk	High
Residual risk (at committee date 2026-09-17)	High: 5 of 8 required evidence areas are not verified: Independent assurance report (Verified with exception or limitation); Access control (Verified with exception or limitation); Subcontractors and subprocessors (Self-reported); Business continuity and recovery (Self-reported); Penetration testing (Verified with exception or limitation)
Target residual if conditions met	Medium (assumption)
Decision	Conditionally approve

2. Evidence by area

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

3. Evidence register

ID	Area	Evidence	Reliance	Period	Gap or exception
VE-001	Independent assurance report	SOC 2 Type II report, managed database hosting service	Independent	2025-07-01 to 2026-03-31	Report period ends 2026-03-31; 6 months (2026-04-01 to 2026-09-30) are not covered and no bridge letter was provided. Disaster recovery site is outside the report's stated scope.
VE-002	Access control	Service auditor test of user access removal (within the SOC 2 report)	Independent	2025-07-01 to 2026-03-31	Exception: 3 of 25 sampled terminated Stratwick personnel had access removed after the vendor's deadline. Vendor management response: tooling fix in Q2 2026; not independently validated.
VE-003	Access control	Complementary user-entity controls (CUECs) listed in the SOC 2 report	Independent	2025-07-01 to 2026-03-31	Six CUECs place duties on Northstar, including timely removal of Northstar users' access to the hosting portal and MFA on Northstar administrator accounts. Project 1 found Northstar leaver removal and MFA failures (F-01, F-05), so the CUECs are not operating effectively on Northstar's side.
VE-004	Encryption	Service auditor test of encryption at rest and in transit (within the SOC 2 report)	Independent	2025-07-01 to 2026-03-31	None noted
VE-005	Retention and deletion	Master services agreement: return and deletion of data on termination	Contractual	2022-04-01 to 2027-03-31	None noted
VE-006	Subcontractors and subprocessors	Subservice organisation list and carve-out statement (within the SOC 2 report)	Self-reported	2025-07-01 to 2026-03-31	Colocation provider is carved out of the report, so its controls are not independently assessed in the evidence provided. Northstar holds no assurance report for the colocation provider.
VE-007	Incident notification	Master services agreement: security incident notification clause	Contractual	2022-04-01 to 2027-03-31	None noted
VE-008	Business continuity and recovery	Disaster recovery failover test summary	Self-reported	2026-02-10 to 2026-02-10	Summary shows failover in 3 h 40 min against Northstar's 4 hour recovery objective (BS-01) but is vendor-prepared and the DR site is outside the SOC 2 scope.
VE-009	Penetration testing	Independent penetration test summary, hosting platform	Independent	2025-11-03 to 2025-11-14	Two medium findings; vendor states both remediated but retest evidence was not provided.

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 the managed hosting service.

Rationale: 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

1. 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)
2. Obtain evidence that the user-access-removal exception was fixed and validated by the service auditor or by Northstar re-performance
3. Obtain independent assurance, or a plan to obtain it, over the disaster recovery site
4. Close Northstar's own leaver-removal and MFA findings (F-01, F-05), because they are the CUECs Northstar must operate
5. 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.

Accountable owner: Head of Payments Engineering. Residual risk acceptance authority: Chief Risk Officer (executive acceptance).

5. Issues

Issue	Area	Severity	Owner	Due	Status	Overdue days
TPR-001	Independent assurance report	High	Stratwick Managed Hosting Inc. (via Head of Payments Engineering)	2026-11-01	Open	0
TPR-002	Access control	High	Stratwick Managed Hosting Inc. (via Head of Payments Engineering)	2026-11-01	In progress	0
TPR-003	Access control	High	IT Security Manager	2026-11-01	In progress	0
TPR-004	Subcontractors and subprocessors	High	Stratwick Managed Hosting Inc. (via Head of Payments Engineering)	2026-11-01	Open	0
TPR-005	Business continuity and recovery	High	Stratwick Managed Hosting Inc. (via Head of Payments Engineering)	2026-11-01	Open	0
TPR-006	Penetration testing	High	Stratwick Managed Hosting Inc. (via Head of Payments Engineering)	2026-11-01	Closed	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.