

SIMULATED CASE STUDY

Vendor Tiering Methodology

Third-party risk

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. Purpose

This method sets how Northstar ranks the inherent risk of a vendor, how deep due diligence goes, how evidence is judged, and how residual risk and decisions follow. All vendors in this exercise are fictional.

2. Inherent risk tiering

Six factors are scored on short ordinal scales and weighted. The scores are an expert-judgement shorthand, not a measurement; they are chosen to separate vendors reasonably and are not calibrated against loss data.

Factor	Scale and points	Weight
Service criticality	Low 1, Medium 2, High 3, Critical 4	x2
Data sensitivity	None 1, Confidential 2, Restricted 3	x2
Privileged connectivity	No 1, Yes 3	x1
Concentration and dependency	Low 1, Medium 2, High 3	x1
Regulatory relevance	Low 1, Medium 2, High 3	x1
Substitutability	Easy 1, Moderate 2, Difficult 3	x1

Weighted total ranges from 8 to 26. Tier 1 (inherent risk High) is 19 or more; Tier 2 (Medium) is 13 to 18; Tier 3 (Low) is 12 or less. Overrides: any Critical service, or Restricted data with privileged connectivity, is Tier 1.

Vendor	Name	Total	Tier	Inherent	Override
V-01	Stratwick Managed Hosting Inc.	26	Tier 1	High	Critical service
V-02	Pinebrook Print and Mail Ltd.	11	Tier 3	Low	
V-03	Lumenvale AI Ltd.	16	Tier 2	Medium	
V-04	Harborview Payroll Services Ltd.	17	Tier 2	Medium	
V-05	Quillon Mail Security Inc.	12	Tier 3	Low	
V-06	Meridian Facilities Group	8	Tier 3	Low	
V-07	Tallowmere Analytics Ltd.	14	Tier 2	Medium	
V-08	Corvid Screening Services Inc.	11	Tier 3	Low	
V-09	Ashgrove Legal Software Ltd.	10	Tier 3	Low	

3. Evidence and reliance

Evidence is judged by who produced it: Independent (service auditor, testing firm), Contractual (a signed term), Self-reported (vendor statement or questionnaire) or None. A questionnaire answer is never independent verification. Evidence not provided is recorded as a gap, not as a control failure: it means the control could not be assessed. An independent report counts only for its stated period and scope, so a report that ends before today, excludes the site Northstar uses, or lists an exception is verified with a limitation, not simply verified.

Tier	Required evidence areas
Tier 1	Independent assurance report; Access control; Encryption; Retention and deletion; Subcontractors and subprocessors; Incident notification; Business continuity and recovery; Penetration testing
Tier 2	Independent assurance report; Access control; Encryption; Retention and deletion; Subcontractors and subprocessors; Incident notification; Business continuity and recovery
Tier 3	Retention and deletion; Subcontractors and subprocessors; Incident notification; Access control

AI service providers are also assessed on model training and data use. An area counts as covered only if it is verified independently or is covered by a clear contractual term; everything else is a gap.

4. Residual risk

Residual risk is assessed separately from inherent risk. Start at the inherent level. If every required area is covered, residual is one level lower. If one area is a gap, residual equals inherent. If two or more are gaps, residual is one level higher (capped at High) because unknowns are treated as risk. The target residual after conditions is a stated assumption that every condition is met and validated.

5. Decisions and acceptance

Outcomes: approve, conditionally approve, restrict or reject. A vendor with High residual risk cannot simply be approved. Restrict and reject decisions list conditions. Residual risk acceptance authority: High residual, the Chief Risk Officer (executive acceptance); Medium, the risk owner; Low, the vendor owner.

6. Monitoring

Tier	Periodic review
Tier 1	Full reassessment every 12 months; quarterly check of issues, incidents and service changes
Tier 2	Evidence refresh every 12 months; full reassessment every 24 months or at renewal
Tier 3	Review at contract renewal or every 24 months, whichever is sooner

Event-driven reassessment triggers: Security incident or breach at the vendor; Qualified or adverse assurance opinion, or a lapsed certificate; Change of ownership, hosting region or subprocessors; Material change to the service, data shared or integrations; Change to retention, training or incident terms; Regulatory or Northstar policy change affecting the service; Overdue critical issue after two escalations.

Issues are tracked with aging, overdue status, closure evidence and a validation result. Overdue 1 to 14 days escalates to the owner's manager, 15 to 30 days to the Head of Procurement, and over 30 days to the risk committee and the Chief Risk Officer. Closure needs validation by Northstar, not only a vendor statement.

7. Limitations

Ordinal scores and weights are the author's judgement. Evidence is scenario content, not real vendor responses. The method has not been tested against real vendor populations, and it does not substitute for legal or privacy advice.