

VENDOR SECURITY ASSESSMENT

Third-party cybersecurity due diligence for a fictional cloud supplier

Sample Portfolio Deliverable | Illustrative Price: \$1,499

FICTIONAL DEMONSTRATION — NOT AN ACTUAL CLIENT REPORT

Executive Summary

Sample vendor: CloudLedger Systems, a fictional SaaS supplier being considered by Northstar Professional Services LLC. The vendor would process confidential business records and receive SSO-based user access.

Sample recommendation: **CONDITIONAL APPROVAL**. Proceed only after the buyer resolves the high-priority evidence gaps below and records accepted residual risk.

Method & Evidence

The structure reflects current NIST cybersecurity supply-chain risk-management guidance. NIST SP 1326 describes due-diligence assessment considerations for ICT suppliers, including provenance, resilience, foundational cyber practices, supply-chain tiers, and foreign ownership/control/influence considerations. This sample adapts those concepts to an SMB vendor review; it is not a substitute for legal, sanctions, procurement or specialized FOCI review.

Evidence Reviewed

- Completed security questionnaire (fictional)
- SOC 2 Type II report summary (fictional)
- Penetration-test executive summary (fictional)
- Business continuity/disaster recovery overview (fictional)
- Incident-response policy summary (fictional)
- Subprocessor list and data-flow description (fictional)

Assessment Summary

Domain	Sample Status	Observation
Governance & ownership	Acceptable	Security responsibilities and annual policy review are documented.
Identity & access	Gap	MFA is required for workforce access, but privileged access-review evidence was not provided.
Vulnerability management	Gap	Scanning is described; remediation SLA evidence is incomplete.

Incident response	Acceptable with follow-up	Plan exists; customer-notification timing should be contractually confirmed.
Resilience	Gap	Backups are described, but recent restore-test evidence was not supplied.
Data protection	Acceptable	Encryption at rest/in transit is stated; key-management evidence should be retained.
Subprocessors / supply chain	Gap	Subprocessor list exists; risk-review cadence is not evidenced.
Assurance evidence	Acceptable	Independent assurance is represented in the sample evidence package.

Open Risks & Required Follow-Up

ID	Issue	Severity	Buyer Follow-Up
VR-01	No evidence of periodic privileged-access review	High	Request latest access-review evidence and exception handling.
VR-02	No recent recovery/restore-test evidence	High	Request latest DR/restore exercise results and corrective actions.
VR-03	Vulnerability remediation SLAs not evidenced	Medium	Request policy/metrics showing critical/high remediation targets.
VR-04	Subprocessor security review cadence unclear	Medium	Request third-party risk process and monitoring frequency.
VR-05	Incident notification requirement not confirmed	Medium	Confirm notification timeline and cooperation duties in contract/DPA.

Decision Record

Decision	Rationale	Conditions
Conditional Approval	Core security program appears plausible in the fictional evidence, but material assurance gaps remain.	Close VR-01 and VR-02 before production data; contractually address notification; track medium findings.

Deliverables

- Vendor security executive summary
- Evidence checklist
- Domain-by-domain assessment

- Risk findings and follow-up questions
- Conditional approval / escalation recommendation
- Residual-risk tracking items

Limitations

A vendor review evaluates supplied evidence and known information; it cannot guarantee that a supplier is secure. Legal, privacy, sanctions, financial viability, procurement and specialized ownership/control reviews may require separate qualified professionals.