Third-party due diligence report

Northwind Sample Supplies LLC · assessed by Example Co. against SOC 2

Sample report. Example Co. and Northwind Sample Supplies LLC are fictional, and so are the people named here. The answers are made up, but every score, control status and audit entry was produced by VendorVett's real scoring engine and report generator.

Vendor

Legal name	Northwind Sample Supplies LLC
Internal reference	VEN-0042
Industry	Inventory management software
Headquarters	Portland, Oregon, United States
Website	https://northwind.example
Business criticality	High
Relationship tier	Preferred
Lifecycle status	Active

Fictional supplier of hosted inventory and order management software. Holds Example Co.'s customer order history and shipping addresses.

Assessment

Questionnaire	Standard Security & Compliance Questionnaire
Framework	SOC 2
Status	Completed
Issued to	security@northwind.example
Sent	01 Sep 2026, 09:14
Submitted by vendor	09 Sep 2026, 16:40
Scored	09 Sep 2026, 16:40
Reviewed and completed	11 Sep 2026, 15:30
Reviewer	Jordan Lee

Risk scores

Scores are risk on a 0–100 scale — higher is riskier — and are produced by a deterministic engine with no AI and no randomness. The same answers always yield the same numbers, and the working is reproduced in full below.

INHERENT RISK

75.00

High risk

RESIDUAL RISK

13.69

Low risk

Method	residual = inherent × (failed_weight / max_weight)

SAMPLE

Inherent basis	Vendor criticality: HIGH
Control weight at stake	126
Weight unattested	23
Gap ratio	18.25%
Scoring engine version	2

SOC 2 control coverage

14 of 19 mapped controls are attested by the vendor's answers. A control counts as attested only when every question mapped to it passed.

Control	Status	Evidence from
A1.2	Attested	Q27. Do you have a business continuity and disaster recovery plan tested in the last 12 months? Q28. Upload evidence of your most recent disaster recovery or failover test.
CC1.2	Attested	Q1. Do you hold a current SOC 2 Type II report or ISO/IEC 27001 certificate? Q2. Upload your most recent SOC 2 report, ISO 27001 certificate, or equivalent.
CC1.3	Attested	Q6. Is a named individual accountable for information security at executive level?
CC1.4	Attested	Q31. Do you run background checks on staff with access to customer data? Q32. Do all staff complete security awareness training at least annually?
CC3.2	Not attested	Q9. Do you carry out data protection impact assessments for new high-risk processing?
CC4.1	Not attested	Q3. When was your most recent independent security audit or certification review? Q18. Do you carry out independent penetration testing at least annually? Q19. Upload the executive summary of your most recent penetration test.
CC5.3	Attested	Q4. Do you maintain documented information security policies, approved by management and reviewed at least annually? Q5. Upload your information security policy, or its table of contents if the full document is confidential.
CC6.1	Attested	Q7. Do you encrypt customer data at rest and in transit? Q8. List the countries where customer data is stored or processed. Q13. Do you enforce multi-factor authentication for all staff access to production systems? Q17. How are production credentials and secrets managed?
CC6.2	Attested	Q14. Is access to customer data granted on a least-privilege basis and reviewed at least quarterly? Q15. Is access revoked within one business day when staff leave or change role?
CC6.3	Attested	Q14. Is access to customer data granted on a least-privilege basis and reviewed at least quarterly?
CC6.5	Attested	Q10. How long do you retain customer data after a contract ends? Q11. Can you delete or export all data for one customer on request, within a defined timeframe?
CC6.6	Attested	Q13. Do you enforce multi-factor authentication for all staff access to production systems?
CC6.7	Attested	Q7. Do you encrypt customer data at rest and in transit?

SAMPLE

Control	Status	Evidence from
CC7.1	Attested	Q20. Do you have a documented vulnerability management process with defined remediation timeframes? Q21. How quickly do you patch critical vulnerabilities in production?
CC7.2	Not attested	Q16. Are privileged and administrative actions logged, retained and reviewed? Q22. Do you monitor systems for security events, with alerting on anomalies?
CC7.3	Attested	Q26. Have you experienced a reportable security breach in the last 36 months?
CC7.4	Attested	Q24. Do you have a documented incident response plan tested in the last 12 months? Q25. How quickly do you commit to notifying customers of a confirmed data breach?
CC9.1	Informational	Q33. Which of the following do you maintain? Q34. Upload a certificate of insurance (general liability or cyber).
CC9.2	Not attested	Q29. Do you use subprocessors that access customer data? Q30. Upload your current subprocessor list.

3 question(s) in this questionnaire are not mapped to a SOC 2 control and are excluded from the coverage figure above. They appear in the response detail.

SAMPLE

Response detail and scoring working

Every question, its outcome, and exactly what it contributed to the residual score. Unanswered scoreable questions fail closed: an unattested control is treated as an open one.

#	Question	Outcome	Weight	Adds to risk
1	Do you hold a current SOC 2 Type II report or ISO/IEC 27001 certificate?	Attested	10	—
2	Upload your most recent SOC 2 report, ISO 27001 certificate, or equivalent.	Informational	—	—
3	When was your most recent independent security audit or certification review?	Informational	—	—
4	Do you maintain documented information security policies, approved by management and reviewed at least annually?	Attested	7	—
5	Upload your information security policy, or its table of contents if the full document is confidential.	Informational	—	—
6	Is a named individual accountable for information security at executive level?	Attested	5	—
7	Do you encrypt customer data at rest and in transit?	Attested	9	—
8	List the countries where customer data is stored or processed.	Informational	—	—
9	Do you carry out data protection impact assessments for new high-risk processing?	Not attested	6	6
10	How long do you retain customer data after a contract ends?	Informational	—	—
11	Can you delete or export all data for one customer on request, within a defined timeframe?	Attested	7	—
12	Upload your data processing agreement or privacy addendum.	Informational	—	—
13	Do you enforce multi-factor authentication for all staff access to production systems?	Attested	8	—
14	Is access to customer data granted on a least-privilege basis and reviewed at least quarterly?	Attested	7	—
15	Is access revoked within one business day when staff leave or change role?	Attested	6	—
16	Are privileged and administrative actions logged, retained and reviewed?	Not attested	5	5
17	How are production credentials and secrets managed?	Informational	—	—
18	Do you carry out independent penetration testing at least annually?	Not attested	8	8
19	Upload the executive summary of your most recent penetration test.	Informational	—	—
20	Do you have a documented vulnerability management process with defined remediation timeframes?	Attested	7	—
21	How quickly do you patch critical vulnerabilities in production?	Informational	—	—

SAMPLE

#	Question	Outcome	Weight	Adds to risk
22	Do you monitor systems for security events, with alerting on anomalies?	Attested	5	—
23	Where does customer data live?	Informational	—	—
24	Do you have a documented incident response plan tested in the last 12 months?	Attested	7	—
25	How quickly do you commit to notifying customers of a confirmed data breach?	Informational	—	—
26	Have you experienced a reportable security breach in the last 36 months?	Attested	8	—
27	Do you have a business continuity and disaster recovery plan tested in the last 12 months?	Attested	6	—
28	Upload evidence of your most recent disaster recovery or failover test.	Informational	—	—
29	Do you use subprocessors that access customer data?	Not attested	4	4
30	Upload your current subprocessor list.	Informational	—	—
31	Do you run background checks on staff with access to customer data?	Attested	6	—
32	Do all staff complete security awareness training at least annually?	Attested	5	—
33	Which of the following do you maintain?	Informational	—	—
34	Upload a certificate of insurance (general liability or cyber).	Informational	—	—
35	Anything else we should know about your security or compliance posture?	Informational	—	—

SAMPLE

Evidence on file

Documents supplied in support of this assessment. Each digest lets a reader confirm that the file they hold is the file that was assessed.

File	Source	Uploaded	SHA-256
northwind-soc2-type2-2026.pdf	Uploaded by the vendor via the portal	08 Sep 2026	`059bdce297a3e57846358d44320eaf7feaf661debb1c9b4eaeeebff853b54368`
northwind-infosec-policy-v4.pdf	Uploaded by the vendor via the portal	08 Sep 2026	`da29d36299bcc33136a668b4474d6f4249cb9dc5f6455d9b7fc2b110e26016d7`
northwind-dpa-2026.pdf	Uploaded by the vendor via the portal	08 Sep 2026	`174c1f5f4916d63d051f23701008edbebea7e186765157db156ed546d5c1253e`

File	Source	Uploaded	SHA-256
northwind-subprocessors.pdf	Uploaded by the vendor via the portal	08 Sep 2026	432330e8af972db4d0de4a0c8791f028dade817755f63f4697bbf307c9c11c3c
northwind-coi-cyber-2026.pdf	Uploaded by the vendor via the portal	08 Sep 2026	3d5be1174b2f118f61e2baba298a86b8bd5a6293334c23f317fb90e76d8992aa

Audit trail

Recorded actions affecting this assessment, its vendor and its evidence, taken from the organization's append-only log. Each entry carries its position in the hash chain, so any line here can be located and verified in the full trail.

#	When	Action	By	Subject
1	01 Sep 2026 09:05	Vendor created	Avery Morgan	Northwind Sample Supplies LLC
2	01 Sep 2026 09:12	Assessment created	Avery Morgan	Northwind Sample Supplies LLC
3	01 Sep 2026 09:14	Assessment sent to vendor	Avery Morgan	Northwind Sample Supplies LLC
4	08 Sep 2026 14:01	Document uploaded	Vendor (portal)	northwind-soc2-type2-2026.pdf
5	08 Sep 2026 14:04	Document uploaded	Vendor (portal)	northwind-infosec-policy-v4.pdf
6	08 Sep 2026 14:11	Document uploaded	Vendor (portal)	northwind-dpa-2026.pdf
7	08 Sep 2026 14:29	Document uploaded	Vendor (portal)	northwind-subprocessors.pdf
8	08 Sep 2026 14:33	Document uploaded	Vendor (portal)	northwind-coi-cyber-2026.pdf
9	09 Sep 2026 16:40	Assessment submitted by vendor	Vendor (portal)	Northwind Sample Supplies LLC
10	09 Sep 2026 16:40	Assessment scored	System	Northwind Sample Supplies LLC
11	10 Sep 2026 10:02	Assessment review started	Jordan Lee	Northwind Sample Supplies LLC
12	11 Sep 2026 15:30	Assessment completed	Jordan Lee	Northwind Sample Supplies LLC

About this report

Responses are the vendor's own attestations. VendorVett records and scores them; it does not independently verify them, and an attested control means the vendor asserted it, not that it was tested. Scores are produced by a deterministic engine (version 2) whose full working is reproduced above. Any AI-generated narrative appears only where a named reviewer accepted it, and is labelled with the model that drafted it.

Generated 11 Sep 2026, 15:45 for Example Co.. Assessment #1042.

SAMPLE