THREATNEXIS | VENDOR RISK MANAGEMENT

Vendor Security Scorecard

A Practical Starter Kit for Evaluating Third-Party Vendor Risk

61%

of 2024 supply-chain attacks originated one hop from the primary vendor (CrowdStrike, 2025 Global Threat Report)

4

vendor risk tiers to help you decide where to focus your limited review time

0–100

scoring scale to track every vendor's security posture over time

FREE EDITION | threatnexis.com | 2026 Edition | For any business that shares data with vendors

What's Inside This Guide

- Why vendor risk is the fastest-growing attack surface
- The business case for a vendor risk program
- The 4-tier vendor risk framework
- A sample Vendor Security Questionnaire (Section 1 of 6)
- A 0–100 vendor scoring rubric
- What's included in the full Premium Toolkit

1. Why Vendor Risk Matters

Every vendor you connect to your systems — your cloud host, your payroll processor, your CRM, even your marketing analytics tool — is a door into your business that you don't fully control. A vendor's weak password policy, unpatched server, or careless employee can expose your data just as easily as a mistake inside your own walls.

Most small and mid-sized businesses have never inventoried which vendors can touch sensitive data, let alone reviewed how well those vendors protect it. That gap is exactly where attackers look first — it's usually easier to compromise a smaller, less-scrutinized vendor than to attack a well-defended target directly.

This guide gives you a practical starting point: how to tier vendors by risk, what to ask them, and how to score what they tell you — without needing a dedicated procurement security team.

> **REAL-WORLD SCENARIO**
>
> A 40-person accounting firm outsourced its client document portal to a third-party SaaS vendor. The vendor left a known vulnerability unpatched for 97 days. Attackers used it to access tax records for over 1,200 clients. The firm had never reviewed the vendor's security practices, and its contract had no breach-notification requirement — the firm learned about the incident from a client, not the vendor. Notification costs, legal fees, and lost clients topped $310,000.

The Business Case for a Vendor Risk Program

Without a Program	With a Program	The Difference
• Vendors onboarded with no security review • Breaches discovered from the vendor's press release • No inventory of who can access sensitive data • Contracts silent on security obligations • Risk discovered only after an incident	• Vendors tiered and reviewed before signing • Breach notification required within 72 hours • Full inventory of vendor data access • Standard security clauses in every contract • Risk reviewed and scored on a fixed cycle	• **Faster breach detection** • **Contractual protection** • **Full data-access visibility** • **Reduced legal & liability exposure** • **Proactive vs. reactive posture**

2. Vendor Risk Tiering Framework

Before assessing any vendor, classify it into a risk tier. The tier determines how deep your review needs to be and how often it repeats — a payroll processor and an office-supplies vendor should never sit on the same review schedule.

FREE FEATURE

Use this framework to triage your full vendor list first. Tier every vendor before you send a single questionnaire — it tells you exactly where to spend your limited review time.

Tier	Criteria	Review Frequency	Example
Tier 1 – Critical	Stores, processes, or transmits regulated/sensitive data, or holds privileged access to core systems	Annual full assessment + quarterly check-ins	Cloud IaaS provider, payroll processor
Tier 2 – High	Has access to internal systems or non-regulated business data	Annual assessment	CRM platform, SSO/IAM provider
Tier 3 – Medium	Limited system access, or handles only public-facing data	Biennial (every 2 years)	Marketing analytics tool
Tier 4 – Low	No data access and no system integration	Assessment on renewal only	Office supplies vendor

PREMIUM FEATURE

Premium extends this framework to your vendors' vendors with a full Fourth-Party Risk Register — 61% of 2024 supply-chain attacks originated one hop removed from the primary vendor, not the vendor itself. Track subprocessor exposure vendor-by-vendor in the Premium Edition.

3. Sample Vendor Security Questionnaire

Send a Vendor Security Assessment Questionnaire (VSAQ) to every Tier 1 and Tier 2 vendor annually, and to all new vendors before contract execution. This free edition includes Section 1 of 6. Review vendor responses with your security lead and score them using the rubric on the next page.

#	Section 1: Organization & Governance	Expected Response Type
1	What security certifications does your organization hold? (SOC 2 Type II, ISO 27001, CSF, HITRUST, etc.)	Open
2	Is there a dedicated CISO or Head of Security? Please provide their name and tenure.	Open
3	How often does your board or executive team receive cybersecurity updates?	Multiple Choice — Monthly / Quarterly / Annually / Never
4	Has your organization experienced a security incident or breach in the last 3 years? If yes, describe the nature, scope, and remediation actions.	Open — Mandatory
5	Do you have a written Information Security Policy reviewed within the last 12 months?	Yes / No / In Progress

PREMIUM FEATURE — 5 MORE SECTIONS, 29 MORE QUESTIONS

The Premium Edition continues with Access Control & Identity, Data Security & Handling, Vulnerability & Patch Management, Incident Response, and Business Continuity — 34 questions total, pre-formatted for distribution straight to vendors.

4. Vendor Scoring Rubric

Score every completed questionnaire from 0–100 based on the completeness and strength of the vendor's responses. Use the band below to decide what happens next.

Score Range	Rating	Recommended Action
90–100	Excellent	Continue standard annual review cycle
75–89	Acceptable	Monitor; request a remediation plan for any gaps
50–74	Needs Improvement	Executive-level review required within 30 days
Below 50	High Risk	Escalate immediately; consider contract review or termination

SCORING NOTE

Score every question the same way each cycle so results are comparable period over period. A vendor whose score drops for two consecutive reviews should be escalated regardless of its absolute score — the Premium Trend Analysis dashboard tracks this automatically across your entire vendor list.