ELEVATE
SOLUTIONS

TEMPLATE · COMPLIANCE & RISK

Vendor Risk Assessment Template

Third-party due diligence

Evaluate a vendor's security posture before they touch your data — aligned with SOC 2 and NIST third-party guidance. Profile the vendor, run the 26-question security questionnaire, score the answers, and route the result through a documented approval chain.

01 — PROFILE

Vendor Profile & Scope

Your vendors are part of your attack surface. Third-party involvement doubled to 30% of breaches. Verizon DBIR 2025 Regulators, clients, and carriers increasingly expect you to show a documented review for every vendor that handles your data — this template is that review.

Two terms drive everything that follows. **Inherent risk** is the risk a vendor relationship carries before you look at their controls: what data they touch, how they connect, and how badly a failure would hurt. **Residual risk** is what remains after you account for the controls they actually run — which is what the questionnaire in Section 02 measures. You set inherent risk in this section through tiering; you measure residual risk in Sections 02–03. Approval decisions are made on residual risk, scoped by tier.

> **HOW TO USE THIS TEMPLATE**
>
> One copy per vendor. Complete Section 01 yourself, send Section 02 to the vendor with the evidence column as a document request list, score per Section 03, then route Section 04 for sign-off. Keep the completed copy with the contract file — it is your audit evidence.

Vendor profile

Vendor name _____

Assessment date _____

Internal owner (relationship) _____

Service / product provided _____

Data types accessed □ Public □ Internal □ Confidential □ Regulated — PHI □ Regulated — PII / NPI □ Privileged / work product

Access method □ SaaS (vendor-hosted) □ Remote access into our network □ API / integration □ On-site personnel □ Data feed only

Approx. users / records in scope _____

Integration points (systems touched) _____

Criticality tier (from table below) □ Tier 1 □ Tier 2 □ Tier 3

Tiering guidance

Assign the highest tier any single criterion triggers. The tier sets review depth, the auto-cap rule in Section 03, and the reassessment cadence in Section 04.

TIER	CRITERIA — ANY ONE TRIGGERS THE TIER	TYPICAL EXAMPLES
Tier 1 Critical	Stores or processes regulated data (PHI, NPI, privileged material); has standing access into your network; outage halts a core business function within 24 hours.	Practice management platform, EHR, cloud file store, IT/MSP provider, payroll
Tier 2 Important	Handles confidential but unregulated data; integrates with a Tier 1 system; outage degrades operations within a week.	CRM, e-signature, marketing platform with client lists
Tier 3 Standard	No access to confidential data or production systems; commodity service with ready substitutes.	Office supplies portal, facilities services, stock-image service

02 — QUESTIONNAIRE

Security Questionnaire — 26 Questions

Send these 26 questions to the vendor. For every "Yes," request the evidence listed — an answer without evidence scores lower (Section 03). Mark **N-A** only where the question genuinely does not apply, and record why.

Questions marked ● are **critical controls**: they carry double weight in scoring, and a "No" on any of them caps the approval outcome (Section 03).

A. Organizational security (Q1–Q4)

#	QUESTION	ANSWER	EVIDENCE REQUESTED
1 ●	Do you hold a current SOC 2 Type II report or ISO/IEC 27001 certification covering the service in scope?	□ Y □ N □ N-A	SOC 2 Type II report (issued within 12 months) or ISO 27001 certificate + Statement of Applicability
2	Is there a designated security officer or equivalent role accountable for your information security program?	□ Y □ N □ N-A	Name/title of security lead; reporting line or charter excerpt
3	Do you maintain written information security policies, reviewed and approved at least annually?	□ Y □ N □ N-A	Policy index with last-review dates and approver
4	Do you carry cyber liability and/or technology errors-and-omissions insurance at limits appropriate to the engagement?	□ Y □ N □ N-A	Certificate of insurance showing coverage type, limits, and policy period

B. Access control (Q5–Q9)

#	QUESTION	ANSWER	EVIDENCE REQUESTED
5 ●	Is multi-factor authentication enforced for all vendor personnel access to systems that store or process our data, including remote and administrative access?	□ Y □ N □ N-A	MFA/SSO enforcement policy or configuration export
6	Is access granted on least-privilege, role-based lines, with our data restricted to personnel who need it for the service?	□ Y □ N □ N-A	Role/permission matrix for the service in scope
7	Do you have documented provisioning and deprovisioning procedures, with departed-employee access removed within a defined timeframe (state it)?	□ Y □ N □ N-A	Joiner/mover/leaver procedure; stated removal timeframe; sample deprovisioning record
8	Are privileged/administrative accounts separated from daily-use accounts, inventoried, and logged?	□ Y □ N □ N-A	Privileged-account inventory; PAM tooling or session-logging description
9	Are user access rights reviewed on a defined schedule (at least annually; quarterly for privileged accounts)?	□ Y □ N □ N-A	Most recent access-review record with date and sign-off

C. Data protection (Q10–Q13)

#	QUESTION	ANSWER	EVIDENCE REQUESTED
10 ●	Is our data encrypted at rest using a current standard (AES-256 or equivalent), with documented key management?	□ Y □ N □ N-A	Encryption standard reference; key-management summary (rotation, custody)
11 ●	Is our data encrypted in transit (TLS 1.2 or higher) on all external and inter-service connections?	□ Y □ N □ N-A	TLS configuration policy or recent external scan result
12	Is our data logically segregated from other customers' data, identifiable on request, and exportable in a usable format?	□ Y □ N □ N-A	Architecture note on tenant segregation; data-export procedure
13	Do you maintain a data retention schedule and perform secure destruction at end of retention, with certificates available?	□ Y □ N □ N-A	Retention schedule; sample destruction certificate

D. Operations security (Q14–Q18)

#	QUESTION	ANSWER	EVIDENCE REQUESTED
14	Do you run a documented vulnerability and patch management program with defined remediation timelines (e.g., critical patches within 14 days)?	□ Y □ N □ N-A	Patch policy with timelines; vulnerability-scan cadence
15	Is endpoint detection and response (EDR) or equivalent deployed on systems that access or process our data?	□ Y □ N □ N-A	EDR product name and coverage statement
16	Are security logs centrally collected, monitored for alerts, and retained for a defined period (state it)?	□ Y □ N □ N-A	Log sources, retention period, and who reviews alerts
17	Do you commission an independent penetration test at least annually, and remediate findings on a tracked schedule?	□ Y □ N □ N-A	Pen-test attestation letter (within 12 months) + remediation summary
18	Do you assess your own subcontractors that touch our data, flow down equivalent security terms, and notify us of material subcontractor changes?	□ Y □ N □ N-A	Subcontractor list for the service; sample flow-down clause; change-notification term

E. Incident response (Q19–Q22)

#	QUESTION	ANSWER	EVIDENCE REQUESTED
19	Do you maintain a documented incident response plan, tested within the last 12 months?	□ Y □ N □ N-A	IR plan table of contents; date and type of last test
20 ●	Will you contractually commit to notifying us of a security incident affecting our data within a defined window (e.g., 72 hours of confirmation)?	□ Y □ N □ N-A	Contract or DPA clause stating the notification window
21	Have you experienced a reportable security incident or breach in the past 36 months? If yes, describe the incident and corrective actions.	□ Y □ N □ N-A	Incident summary and corrective-action report (“Yes” with strong remediation can still score — see Section 03 note)
22	Do you provide a designated incident contact and an intake channel monitored around the clock for security reports?	□ Y □ N □ N-A	Escalation contact and intake channel (phone/portal/email)

F. Business continuity (Q23–Q26)

#	QUESTION	ANSWER	EVIDENCE REQUESTED
23	Do you maintain documented business continuity and disaster recovery plans with stated RTO and RPO targets for the service in scope?	□ Y □ N □ N-A	BCP/DR document excerpt showing RTO/RPO values
24 ●	Are backups of our data performed on a defined schedule, and is restoration tested at least annually with results recorded?	□ Y □ N □ N-A	Backup schedule; most recent restore-test record with outcome
25	Have you run a disaster recovery exercise within the last 12 months, with findings tracked to closure?	□ Y □ N □ N-A	DR exercise report: date, scenario, findings, closure status
26	Can you demonstrate financial viability for the contract term, and do you offer source-code escrow or a contractual data-return commitment on insolvency or termination?	□ Y □ N □ N-A	Financial summary or D&B report; escrow agreement or data-return clause

03 — SCORING

Risk Scoring Matrix

Score every answered question 0–2, double the points on the six ● critical questions, divide by the maximum applicable, and read the action off the thresholds table. The arithmetic is deliberately simple enough to defend in an audit.

Step 1 — Score each answer

ANSWER	POINTS	RULE
Yes, with evidence provided	2	The requested evidence was received and supports the claim.
Yes, attestation only	1	Vendor answered Yes but did not produce the requested evidence.
No	0	Control absent, or answer left blank after follow-up.
N-A (justified)	—	Excluded from both earned points and maximum. Justification recorded.

Q21 exception: Q21 asks about past incidents, so "No incidents" scores 2; "Yes" with a credible corrective-action report scores 1; "Yes" with no remediation evidence scores 0.

Step 2 — Apply weights and compute the percentage

The six critical questions (Q1, Q5, Q10, Q11, Q20, Q24) carry weight 2; the remaining twenty carry weight 1. Maximum possible score with all 26 applicable: (20 × 1 + 6 × 2) × 2 = **64 points**. For each N-A question, subtract its maximum (2 for standard, 4 for critical) from the denominator.

> FORMULA
>
> Residual risk score % = (sum of weight × points earned) ÷ (maximum applicable points) × 100

Step 3 — Read the action off the thresholds

SCORE	RISK RATING	ACTION
85–100%	**Low**	**Approve.** Standard contract terms; reassess on the tier cadence in Section 04.
70–84%	**Moderate**	**Approve with conditions.** List each gap, the compensating control or remediation owner, and a due date in the sign-off block.
50–69%	**Elevated**	**Remediate before approval.** Vendor closes the identified gaps; re-run the affected questions and re-score before any data access.
Below 50%	**High**	**Reject** — or obtain written executive risk acceptance with a stated expiry date and compensating controls.

AUTO-CAP RULE

A "No" on any ● critical question caps the outcome regardless of total score: at **"Remediate before approval"** for Tier 1 vendors, and at **"Approve with conditions"** for Tier 2 and Tier 3. Missing MFA or encryption is not offset by good paperwork elsewhere.

Worked example

Tier 1 vendor; Q18 is N-A (no subcontractors touch the data), so the denominator is 64 − 2 = **62**. All six critical questions are Yes with evidence: 6 × 2 × 2 = 24. Of the 19 applicable standard questions, 12 are Yes with evidence (24), 4 are attestation-only (4), 3 are No (0): 28. Total 52 ÷ 62 = **83.9% → Moderate → Approve with conditions** — the three No answers and four unevidenced answers become the conditions list, each with an owner and due date. No critical question was a No, so the auto-cap does not apply.

Likelihood × impact check

As a sanity check on the arithmetic, place the vendor on this matrix. **Likelihood** comes from the score (85%+ = Low, 70–84% = Medium, below 70% = High). **Impact** comes from Section 01 (Tier 1 or regulated data = High, Tier 2 = Medium, Tier 3 = Low). If the matrix says Critical but the thresholds said Approve, re-check the tiering — the inherent risk is probably understated.

LIKELIHOOD ↓ / IMPACT →	LOW IMPACT	MEDIUM IMPACT	HIGH IMPACT
Low (score 85%+)	Low	Low	Moderate
Medium (70–84%)	Low	Moderate	High
High (below 70%)	Moderate	High	Critical

Points earned _____

Maximum applicable _____

Score % _____

Risk rating / outcome □ Low — Approve □ Moderate — Approve w/ conditions □ Elevated — Remediate □ High — Reject

04 — APPROVAL

Approval Workflow

A score without a sign-off chain is an opinion. Four roles sign in order; no data access is provisioned until the final approver signs. One person may hold two roles, but the assessor and final approver must be different people.

Sign-off chain

ROLE	RESPONSIBILITY	NAME & TITLE	DATE / DECISION
1. Requestor	Business sponsor. Confirms the service need and the Section 01 profile is accurate.		
2. Assessor	Runs the questionnaire, validates evidence, computes the score, drafts conditions.		
3. Data owner	Owner of the data classification in scope. Confirms the tier and accepts any conditions affecting their data.		
4. Final approver	Management or compliance. Signs the outcome; only role authorized to record a risk acceptance.		

Conditions / remediation items (owner + due date each) _____

_____

_____

Reassessment cadence

TIER	SCHEDULED REASSESSMENT	SCOPE
Tier 1	Annually	Full questionnaire, fresh evidence (do not roll forward last year's SOC 2).
Tier 2	Every 2 years	Full questionnaire; evidence refresh on critical questions only in the off year.
Tier 3	Every 3 years or at contract renewal	Profile review; questionnaire only if the tier changed.

Out-of-cycle triggers — reassess immediately, regardless of tier: the vendor reports a security incident; the service scope or data classification changes; a material subcontractor change is disclosed (Q18); the vendor is acquired or restructures; an audit report (SOC 2 / ISO) lapses or is qualified.

Offboarding / termination checklist

Run this within 30 days of contract end or termination for cause. The vendor file stays open until all five items are checked.

- [ ] **Revoke all access** 1
  Disable vendor accounts, API keys, VPN profiles, and SSO assignments; remove firewall rules and remote-access entries tied to the vendor.
- [ ] **Data return and destruction certificate** 2
  Receive your data in the agreed export format, then obtain a written destruction certificate covering production data and backups, with dates.
- [ ] **Close BAA / DPA obligations** 3
  Confirm the business associate or data processing agreement's termination duties are satisfied and documented; file the closure with the contract.
- [ ] **Rotate shared credentials and secrets** 4
  Change any passwords, service-account credentials, certificates, or encryption keys the vendor ever held or could have observed.
- [ ] **File lessons learned** 5
  Record what worked, what didn't, and any questionnaire questions this vendor exposed as weak — feed it into the next assessment cycle.

Offboarding completed by / date _____

ELEVATE SOLUTIONS

Elevate Solutions provides managed IT and cybersecurity for businesses that answer to regulators, clients, and courts.

Elevate Solutions

6230 Wilshire Blvd Suite 2120, Los Angeles CA 90048

(424) 400-6625 · support@elevatesolutions.io · elevatesolutions.io