SECURITY · TEMPLATE

Vendor Risk *Scoring* for Regulated SMBs

KAANSYSTEMS.COM/LIBRARY/VENDOR-RISK-SCORING · JULY 29, 2026

ABOUT THIS TEMPLATE

Your security floor is your vendors' security floor. Most SMBs assess vendors by gut feel. A four-factor rubric turns that into a repeatable score that tells you who to review and how often.

THE TEMPLATE

Score each vendor across the four factors. Multiply data sensitivity by nothing — just sum — but if you want the sensitivity to dominate, weight Factor 1 double. Keep it simple enough that you'll actually run it.

VENDOR	DATA SENSITIVITY (1-3)	ACCESS DEPTH (1-3)	ATTESTATION GAP (1-3)	BLAST RADIUS (1-3)	SCORE (4-12)	TIER	NEXT REVIEW
Example: analytics vendor	2	2	1	2	7	High	+ annual
Example: PHI data processor	3	3	2	3	11	Critical	+ annual
Example: image CDN	1	1	1	1	4	Low	at change

Tier thresholds

- 10-12 Critical — procurement review + annual + contract notification clause + sub-processor list
- 7-9 High — procurement review + annual + attestation on file
- 5-6 Medium — procurement review + re-review on material change

- 4 Low — lightweight check at procurement

Scoring rules

- Score at procurement, before access is granted, and record the score.
- Re-score any vendor immediately if they disclose a breach — a Critical vendor's incident is your incident.
- The sub-processor list on your trust page is the source of truth for who touches customer data; every vendor scoring on Factor 1 at 2+ belongs on it.

HOW TO USE IT

Score at the gate, not after. The cheapest time to assess a vendor is before you've integrated them, when "no" is still easy and you have leverage to ask for the DPA, the attestation, or the notification clause. A vendor scored after they're wired into production is a vendor you're stuck with. Make the score a required field on the procurement checklist.

Re-score on their breach, not just your calendar. The annual cadence is the floor. The real trigger for a re-score is a vendor disclosing an incident of their own — that's the moment their risk to you changed, and it's exactly when most SMBs do nothing because there's no process pointing at it. A Critical-tier vendor's breach notification should automatically open a review on your side.

The rubric's job is triage, not certainty. A four-factor score won't tell you a vendor is safe. It tells you which five vendors out of forty deserve the deep review your team actually has time for, and which thirty-five don't. That triage is the whole value: it turns "review all our vendors" — a task that never happens — into "review the five that matter," which does.