anchor@anchor-cyber:~$ man vendor-risk

ANCHOR CYBER SECURITY LLC

Vendor / Third-Party Risk

Anchor's own TPRM service line, condensed: tiering, the pre-signature checklist, and the questions that actually separate a real security program from a filled-out questionnaire.

$ tprm --tier

Criticality Tiers / depth of review scales with tier, not vendor size

Low

No access to sensitive data or production systems. E.g. a marketing tool with only public info.

`review: at renewal`

Moderate

Limited access to internal (non-regulated) data, or a dependency for a non-critical function.

`review: annual`

Critical

Access to regulated data (PHI/PII/PCI) or a dependency whose outage stops the business. This is where a BAA/DPA is non-negotiable.

`review: annual + monitor continuously`

$ tprm --pre-signature

Before Anyone Signs Anything

- ☐ Criticality tier assigned *before* the security review starts — this decides how deep to go, not the vendor's sales rep
- ☐ Security questionnaire completed (SIG Lite for moderate, full SIG or CAIQ for critical/cloud vendors)
- ☐ BAA executed before any regulated data (PHI) is shared — not after, not "in progress"
- ☐ DPA executed if the vendor processes personal data subject to GDPR/CCPA
- ☐ Subprocessor list reviewed — a vendor's own subprocessors inherit the same tier logic
- ☐ Breach notification clause with a specific time window, not "promptly" left undefined
- ☐ Right-to-audit or right to request a SOC 2 / ISO 27001 certificate, for critical-tier vendors
- ☐ Data deletion/return terms on contract termination — decided now, not negotiated during an offboarding dispute

$ tprm --red-flags

Red Flags in a Completed Questionnaire

- ✕ Every answer is "Yes, fully compliant" with zero exceptions or in-progress items — a real security program has known gaps and says so.
- ✕ SOC 2 report offered is Type I, not Type II, for a critical-tier vendor — Type I only proves controls exist on one day, not that they operate over time.
- ✕ Vendor can't name their own subprocessors, or the list is stale relative to their own privacy policy.
- ✕ "We'll sign the BAA after go-live" — this is a compliance gap being scheduled, not resolved.
- ✕ No named security contact — questionnaire answers came from sales, not security or engineering.

src: Anchor TPRM service line · SIG/CAIQ questionnaire practice exit 0