



THIRD-PARTY RISK

From annual to continuous.

Six moves that retire the once-a-year questionnaire, the spreadsheet of contract dates, and the six-week evidence hunt. None of them require our product. All of them are faster with it.

- 1 Pick one standard question set and map it once.**
Every vendor answers the same bank (operations, security, compliance, best practices, AI governance), mapped to SOC 2, HIPAA, HITRUST, ISO 27001, NIST and the EU AI Act. Answers become comparable; one answer serves every framework you report to.
- 2 Make vendor status a gate in procurement.**
"Assessing" means not yet cleared to touch regulated data. "Approved" releases them. Criticality and risk rating decide how deep the review goes: the identity provider gets the full bank, the observability tool gets the short one.
- 3 Put every agreement in one register with reminders.**
BAA, DPA, MSA, NDA, with the executed document attached and the owner reminded at 30, 14 and 7 days. Link each agreement to the vendor and, where relevant, to the AI system it covers.
- 4 Stand up the AI inventory this quarter.**
Every AI system your vendors supply and your teams built, classified by risk, with an owner for human oversight, the evaluations passed, the DPIA status and what data it touches. Even a list beats none.
- 5 Define "material change" and re-assess on that, not the calendar.**
A model swap, a new sub-processor, a new agent capability, a breach or a lapsed SOC 2 is a material change to what you approved. Re-assess then, not next spring.
- 6 Collect evidence continuously.**
Policies, personnel, agreements and dispositioned findings accumulate against the record all year, so the audit becomes an export, not a project.

WHAT COUNTS AS A MATERIAL CHANGE

- New or changed model, hosting provider or sub-processor
- Agent gains a new capability (write, execute, spend)
- SOC 2 or ISO certificate expires or scope changes
- Breach, incident or regulator notice at the vendor
- New data category shared (PHI, PCI, CUI)
- Ownership change, acquisition or key-person departure

HOW KOLLGUARD RUNS THE SIX MOVES

- Standard question bank with readiness rings per vendor
- Status as a control on the vendor register, overdue reviews on the row
- Agreement register with 30/14/7-day reminders and a daily digest
- AI inventory with ISO 42001, NIST AI RMF and EU AI Act classification
- Vendor Watch: breach alerts and SOC 2 verification, automatically
- Evidence packages and a hash-chained audit log, exportable any day

Time to stand up: vendor register and agreements from a CSV in an afternoon; the first questionnaire the same day. Vendors do not need another portal: paste their SOC 2, SIG or CAIQ, or send a share link.

ON STAGE IN 2026 Where KollGuard has pitched, exhibited and sponsored this year · kollguard.com/spotlight

JUL 18–19
AGI Summit

Startup track · customer exchange

JUL 30 – AUG 1
Stanford AI Summit

Exhibitor · main-stage pitch

AUG 26–27
Step SF

Spotlight Startup · pitch competition

SEP 17–18
ISACA Sacramento 2026

Platinum sponsor · speaker session