Third-Party Risk Management

Discovery question checklist: Questions that reveal real vendor risk

How to use this checklist

Standard questionnaires tell you what a vendor says it does. This checklist is designed to reveal what the vendor actually does, where it is weakest and how it behaves under pressure. Use it in discovery calls and workshops and follow up with evidence requests.

- **Tier first.** Match depth to criticality. Use all sections for critical vendors, sections 1 to 4 and 6 for medium-risk vendors, and a short form for low-risk suppliers.
- **Ask for proof.** Ask **"show me"** and **"walk me through the last time"**, **NOT** **"do you have"**. Specific examples are harder to rehearse than policy statements.
- **Involve the right people.** Put security, procurement, legal, privacy and the business owner in the room. Risks often sit in the gaps between functions.
- **Record as you go.** Tick each question as covered. Score the answer using the key below and record the evidence reference.

Scoring key

Rating	Meaning	Typical action
Green	Specific answer, supported by evidence	Accept and file the evidence
Amber	Plausible but unevidenced, partial or dated	Request evidence; set a deadline; consider a contractual commitment
Red	Evasive, contradictory or control absent	Escalate; require remediation plan before onboarding, or reconsider the vendor

Vendor details

Vendor name		**Date of discovery**	
Service provided		**Business owner**	

KOOTEK

Risk tier (critical / high / medium / low)		**Assessor(s)**	



Discovery questions

1. Business context and criticality

Start here. Inherent risk comes from what the vendor does for you, not from how polished their questionnaire is.

	Discovery question	What a strong answer looks like	Red flags to probe
A	**What exactly will the vendor do for us, and which of our processes stop if they fail?**	Business owner can name the process, its impact and a tolerable outage window.	Vague scope; nobody internally can say what depends on the vendor.
B	**What data, systems or customers will the vendor touch, and at what volume?**	Specific data categories, volumes and systems documented before onboarding.	“Minimal” or “none” with no evidence; scope that grows after contract signature.
C	**Is the vendor a sole source, or could we switch within a defined period?**	Alternatives identified, switching time estimated and tested on paper.	No alternative and no exit plan; dependency discovered only after go-live.
D	**Will the vendor act on our behalf, speak to our customers or hold our credentials?**	Delegation is explicit, limited and approved by a named owner.	Vendor can make changes or contact customers without our oversight.
E	**How long has the vendor delivered this service to organisations like ours?**	Verifiable references in the same sector and of similar scale.	References are only friendly contacts; no comparable clients.

2. Governance and accountability

Who is accountable tells you more than which policies exist.

	Discovery question	What a strong answer looks like	Red flags to probe
A	**Who in your leadership owns information security, privacy and operational resilience, and who do they report to?**	Named executive with board visibility and an independent reporting line.	Security reports into IT delivery only; the role is vacant or part-time.
B	**How often are policies reviewed, and when did your board last review cyber risk?**	Annual review at minimum with dated approvals and minuted board discussion.	Policies undated or unchanged for years; no board-level reporting.

	Discovery question	What a strong answer looks like	Red flags to probe
C	**What is your internal audit and risk programme, and what were the most significant findings last year?**	Candid summary of findings, owners and remediation status.	“No significant findings” year after year; defensive or evasive answer.
D	**Which independent certifications or attestations do you hold, and what is the exact scope?**	Current ISO 27001, SOC 2 Type II or Cyber Essentials Plus with scope covering our service.	Certificate covers one office or product only; expired or “in progress” for long periods.
E	**Have you had any qualified opinions, major non-conformities or exceptions in recent audits?**	Open disclosure with remediation evidence.	Refusal to share reports under NDA; heavily redacted summaries only.

3. Information security controls

Ask for how controls operate in practice, not whether they exist.

	Discovery question	What a strong answer looks like	Red flags to probe
A	**How do you identify, prioritise and patch vulnerabilities, and what are your target timescales for critical issues?**	Defined SLAs, tooling and metrics, with evidence of actual performance.	No SLAs; “we patch regularly”; large backlog of overdue critical items.
B	**When did you last run an independent penetration test, and how were the findings closed?**	Test within 12 months, executive summary available, remediation tracked.	Tests are internal only; findings still open from previous cycles.
C	**How is data encrypted in transit and at rest, and who holds and rotates the keys?**	Modern standards, documented key management, customer-managed keys where needed.	Shared keys, no rotation, or encryption described only as “industry standard”.
D	**Describe your secure development lifecycle, including code review, dependency scanning and secrets management.**	Automated scanning in pipelines, peer review and a software bill of materials.	Developers hold production access; secrets stored in code or tickets.
E	**How do you detect and respond to threats, and is monitoring 24/7?**	Central logging, alerting, defined response roles and tested playbooks.	Monitoring relies on one individual or office hours only.
F	**How is our data separated from your other customers’ data?**	Logical or physical separation with tested tenant isolation.	Shared environments with unclear segregation.

4. Access and identity

Most real-world vendor compromises start with credentials.

	Discovery question	What a strong answer looks like	Red flags to probe
A	**How do you enforce multi-factor authentication for staff, administrators and service accounts?**	Phishing-resistant MFA for privileged and remote access, with no exceptions list.	MFA optional for some users; shared admin accounts.
B	**Who at your company can access our data, and how is that access approved, reviewed and removed?**	Role-based access, quarterly reviews, same-day leaver removal, full logging.	Broad support access “as needed”; no periodic recertification.
C	**Do you use contractors or offshore teams with access to our data or environment?**	Fully disclosed locations, vetting standards and contractual flow-down.	Hesitation or inconsistent answers about who has access and from where.
D	**How are privileged sessions recorded, and how do you control customer-support access to production?**	Just-in-time elevation, session recording and customer notification options.	Standing administrator rights; support staff can view customer data freely.
E	**How do staff receive security training, and how do you test it?**	Role-specific training, phishing simulations and tracked completion.	Annual click-through only; no measurement.

5. Data handling and privacy

Under UK GDPR you remain accountable for your data even when a vendor processes it.

	Discovery question	What a strong answer looks like	Red flags to probe
A	**Where will our data be stored, processed and accessed from, including backups and support locations?**	Complete list of countries with legal transfer mechanism for each.	Answer covers only primary hosting; remote support locations unmentioned.

	Discovery question	What a strong answer looks like	Red flags to probe
B	**Will you use our data for any purpose beyond delivering the service, including analytics or training models?**	Clear contractual prohibition, or explicit opt-in with controls.	Broad licence language; “aggregated” or “anonymised” use without definition.
C	**How long do you retain our data, and how do you prove deletion at contract end?**	Defined retention schedule, deletion certificates, backup expiry timescales.	No deletion process; data kept indefinitely “for legal reasons” without specifics.
D	**How do you support data subject requests and notify us of requests you receive directly?**	Documented process with agreed timescales.	No process or reliance on us to chase.
E	**Who is your data protection officer or privacy lead, and when was your last DPIA or privacy audit?**	Named contact, current records of processing, evidence of recent assessments.	No privacy lead; records of processing missing.

6. Fourth parties and supply chain

Your vendor’s vendors are your risk too. Ask who sits underneath the service.

	Discovery question	What a strong answer looks like	Red flags to probe
A	**Which subprocessors and critical suppliers support the service, and what do they do with our data?**	Current subprocessor list, with notice and objection rights for changes.	No list available; list found only on a web page that changes without notice.
B	**How do you assess and monitor your own critical suppliers?**	Tiered programme, evidence reviews and exit plans for key suppliers.	“We trust our partners”; no assessment evidence.
C	**Which cloud providers and key software components does the service depend on?**	Dependencies mapped, including regional hosting and open-source components.	Unable to describe dependencies beyond the main cloud provider.
D	**What happens to our service if a critical fourth party fails or is breached?**	Documented contingency, contractual flow-down and notification duties.	Never considered; no contractual obligations on subcontractors.
E	**Have you had to replace a critical supplier in the last three years, and how did it go?**	Concrete example with lessons learned.	Cannot give an example, suggesting untested plans.

7. Resilience, continuity and concentration

Test whether continuity plans have ever met reality.

	Discovery question	What a strong answer looks like	Red flags to probe
A	**What are your recovery time and recovery point objectives for our service, and when did you last prove them?**	Targets documented, tested at least annually, results shared.	Targets are aspirational; no test within the past year.
B	**Describe your last significant outage: cause, duration, customer impact and changes made afterwards.**	Candid post-incident review with corrective actions.	Claims of no outages in several years; defensive or generic answer.
C	**Are your primary and backup environments truly independent, including people and suppliers?**	Separate regions or providers, tested failover, immutable backups.	Backups in same account and region; failover never tested.
D	**How would you operate if key staff or your main site were unavailable?**	Cross-trained teams, documented succession and remote capability.	Key-person dependency on one or two individuals.
E	**Does your service share a common dependency with many other vendors we use?**	Vendor understands and discloses concentration risk.	Unaware of shared dependencies such as the same cloud region.

8. Incidents and breach history

How a vendor behaves when things go wrong predicts how they will treat you.

	Discovery question	What a strong answer looks like	Red flags to probe
A	**Have you suffered a security incident, ransomware event or data breach in the last three years?**	Open, factual account of what happened and what changed.	Flat denial with no supporting evidence; or minimising language.
B	**What is your process and timescale for notifying customers of an incident affecting them?**	Contractual notification window measured in hours, with named contacts.	Notification only when legally required or after investigation concludes.
C	**Do you have cyber insurance, and what are the limits and exclusions?**	Cover proportionate to the data and service, with confirmation available.	No cover, or limits far below potential impact.

	Discovery question	What a strong answer looks like	Red flags to probe
D	**Have you been subject to any regulatory investigation, enforcement action or significant complaint?**	Full disclosure, with outcomes and corrective action.	Reluctance to discuss; public records contradict their answer.
E	**How do you test incident response, and which customers have participated?**	Annual exercises including leadership; customers invited for relevant scenarios.	Plan exists on paper but has never been exercised.

9. Financial health and viability

A vendor that runs out of money often cuts security first.

	Discovery question	What a strong answer looks like	Red flags to probe
A	**Can you share recent audited accounts, and how many months of runway do you have?**	Accounts available, healthy cash position or credible funding.	Late filings, going-concern warnings or no willingness to share.
B	**How dependent are you on a small number of customers, investors or products?**	Diversified revenue with no single customer dominating.	Material reliance on one customer or a single product line.
C	**Are there any planned acquisitions, mergers, restructures or major redundancies?**	Transparent about changes and their impact on service and support.	Sudden leadership departures or unexplained layoffs in engineering or security.
D	**What would happen to our service and data if you ceased trading?**	Escrow, data return commitments and continuity arrangements.	No plan; contract silent on insolvency.

10. Legal, regulatory and ethical conduct

Reputational risk travels up the supply chain to you.

KOOTEK

	Discovery question	What a strong answer looks like	Red flags to probe
A	**Which regulations apply to you and how do you evidence compliance, for example UK GDPR, FCA or NIS expectations and sector rules?**	Mapped obligations with named owners and evidence.	“We are compliant” without detail.
B	**Do you comply with the Modern Slavery Act and how do you assess labour practices in your supply chain?**	Published statement, due diligence and corrective action examples.	No statement; no visibility beyond tier-one suppliers.
C	**What anti-bribery, sanctions and conflict-of-interest controls do you operate?**	Policy, training, screening and gifts register in active use.	No screening of third parties or beneficial owners.
D	**Who are your ultimate beneficial owners, and are any subject to sanctions or political exposure?**	Transparent ownership structure available on request.	Opaque offshore ownership with no explanation.
E	**Are there any ongoing litigation, claims or disputes that could affect our service?**	Clear disclosure with impact assessment.	Material disputes discovered later through public searches.

11. AI and emerging technology

Increasingly, vendors embed AI into services without telling customers.

	Discovery question	What a strong answer looks like	Red flags to probe
A	**Does the service use AI or machine learning, including third-party models, and where?**	Complete inventory of AI features with providers named.	Features added silently; no AI governance owner.
B	**Is our data sent to AI providers, retained by them or used to train models?**	Contract terms prohibit training and retention, with technical enforcement.	Default opt-in to training; unclear flow of prompts and outputs.
C	**How do you control what AI agents or automations can access and do on our behalf?**	Unique identities, least privilege, human approval for high-impact actions, full logging.	Agents share accounts or hold broad standing access.
D	**How do you test AI for prompt injection, data leakage, bias and unreliable outputs?**	Documented testing, red teaming and ongoing monitoring.	Reliance on provider assurances alone; no testing evidence.
E	**Which AI governance framework or standard do you align to?**	Alignment to NIST AI RMF, ISO/IEC 42001 or similar, with ownership defined.	No framework; policy exists only as a marketing statement.

12. Exit, termination and ongoing oversight

Risk management does not end at signature. Make sure the contract lets you act.

	Discovery question	What a strong answer looks like	Red flags to probe
A	**What is your exit process, and how will you return or delete our data in a usable format?**	Documented, tested exit plan with defined timelines and formats.	Proprietary formats only; deletion at vendor's discretion.
B	**What audit, assurance and information rights will we have under the contract?**	Right to audit or receive independent reports, plus change notifications.	Audit rights refused or limited to annual self-assessments.
C	**What service levels apply, and what are the real remedies for missing them?**	Measurable SLAs, reporting and meaningful credits or termination rights.	SLAs without remedies; vendor-controlled reporting only.
D	**How will you notify us of material changes in ownership, subprocessors, locations or security posture?**	Contractual notice periods with right to object or terminate.	Changes announced after the fact.
E	**Who is our named relationship owner on your side, and how often will we review performance and risk?**	Named contacts and scheduled reviews with agreed metrics.	Support is ticket-only; no relationship governance.

Verify, then trust

Answers are only the starting point. These checks help separate confident claims from reliable ones:

- **Cross-check evidence.** Compare what the vendor tells you with certificates, audit reports, trust pages and public records. Scope gaps are common.
- **Look outside-in.** Use external ratings, breach databases, Companies House filings and news searches to test their narrative. Treat ratings as prompts for questions, not verdicts.
- **Interview more than one person.** Ask a technical person and a commercial person the same question. Differences reveal where the story is thin.
- **Turn gaps into commitments.** Where a risk is accepted, convert it into a contractual obligation, a deadline or a monitored metric.
- **Keep reviewing.** Reassess critical vendors at least annually, and whenever ownership, scope, data types or technology change.

Ten patterns that usually signal hidden risk

- Certification scope that excludes the service you are buying.
- Answers that describe policy but never a real example.
- Reluctance to name subprocessors, locations or contractors.
- A claim of zero incidents, outages or findings over several years.
- No tested exit plan, backup restoration or incident exercise.
- Security ownership sitting several layers below leadership.
- Broad internal access to customer data “to help support”.
- Unexplained use of AI features or customer data for model training.
- Financial strain combined with falling investment in security.
- Resistance to audit rights, notification duties or evidence requests.