

Third-Party Risk Lead: senior interview pack

Owning supplier risk when the business has already signed, evidence is partial and fourth parties matter. Free from thallanaresh.com. Answers are outlines to adapt with your own examples.

The contract was signed before the assessment

A business unit signed a three-year contract with a data analytics vendor and only then sent you the questionnaire. The vendor will process customer data next week.

Situation read: You have lost contract leverage, but you can still shape onboarding and data flows.

What I'd do first: Do a rapid assessment of the riskiest points (data handling, access, breach notification), and limit data shared until the gaps are known.

Trade-offs: Delaying go-live upsets the business; going ahead blind creates exposure you own.

What I'd tell leadership: I would allow a restricted start with conditions and dates, and propose a procurement gate so contracts cannot be signed without risk sign-off.

What interviewers listen for

- Works with the situation as it is
- Uses data minimisation as a control
- Fixes the process upstream

Every critical supplier uses the same cloud region

Mapping fourth parties, you find most of your critical suppliers depend on the same cloud provider and region.

Situation read: Each supplier looks resilient alone, but together they create concentration risk you never assessed.

What I'd do first: Confirm the dependency with the suppliers, model the impact of that region failing, and identify which services have tested failover.

Trade-offs: Asking suppliers to change hosting is costly and may be refused; accepting the risk needs explicit approval.

What I'd tell leadership: I would present the concentration as an enterprise risk with options (multi-region requirements at renewal, exit plans, acceptance) for leadership to decide.

What interviewers listen for

- Thinks beyond single-vendor assessments
- Quantifies a shared-failure scenario
- Takes it to enterprise risk

Suppliers stop answering your questionnaires

Response rates fall sharply. Suppliers complain your questionnaire is long and duplicates their published trust materials.

Situation read: Long, uniform questionnaires waste effort on low-risk suppliers and produce poor answers from high-risk ones.

What I'd do first: Tier suppliers by data and access, accept standard reports and trust-centre evidence for lower tiers, and keep targeted questions for critical ones.

Trade-offs: Reducing questions may miss something; keeping them all gets ignored.

What I'd tell leadership: I would show leadership coverage and turnaround improving, with deeper reviews concentrated where the exposure is.

What interviewers listen for

- Right-sizes assessment to risk
- Uses existing assurance
- Measures programme effectiveness

A vendor's breach is in the news but they are silent

Media report a breach at a payroll vendor you use. The vendor has not contacted you, and its account manager is not responding.

Situation read: Your contractual notification right may not have been triggered yet, but your employees' data could be exposed.

What I'd do first: Invoke the incident contact path in the contract, assess what data the vendor holds, and prepare internal communication with HR and legal.

Trade-offs: Acting on press reports risks overreacting; waiting risks late response to your own obligations.

What I'd tell leadership: I would brief leadership on what is known and unknown, our likely notification duties, and the escalation steps taken with the vendor.

What interviewers listen for

- Knows contract notification terms
- Acts on partial information carefully
- Coordinates legal and HR

Your most critical vendor fails the review

A sole-source supplier for a core service fails several control areas. Replacing it would take over a year.

Situation read: Terminating is not realistic; the job is to reduce exposure while keeping service.

What I'd do first: Agree a remediation plan with dates and evidence, add compensating controls on your side, and start exit planning in parallel.

Trade-offs: Pushing hard may sour a relationship you depend on; going soft leaves the gaps open.

What I'd tell leadership: I would recommend formal risk acceptance for a defined period, with a remediation plan, quarterly check-ins and a funded exit option.

What interviewers listen for

- Avoids unrealistic all-or-nothing answers
- Combines remediation, compensating controls and exit
- Time-boxes acceptance

A vendor relationship ended but the data did not

A marketing vendor was dropped a year ago. An access review shows its integration keys still work and it still holds customer records.

Situation read: Offboarding was treated as a commercial event, not a security one.

What I'd do first: Revoke credentials immediately, request a certificate of deletion, and check logs for any use after termination.

Trade-offs: Legal escalation takes time; a friendly request may be ignored.

What I'd tell leadership: I would report the incident path, add offboarding steps to the vendor lifecycle, and run a sweep for other ended vendors with live access.

What interviewers listen for

- Treats offboarding as a control
- Acts on credentials first
- Looks for the pattern, not one case

A vendor quietly starts training AI on your data

A vendor updates its terms to allow using customer data to improve its AI models. The change was buried in a release note.

Situation read: This changes the data processing purpose and may conflict with your commitments to customers.

What I'd do first: Check the contract's change and data-use clauses, ask the vendor for an opt-out in writing, and assess what data is affected.

Trade-offs: Switching vendors is disruptive; accepting may breach your own privacy commitments.

What I'd tell leadership: I would tell leadership the exposure and the options, and add AI data-use terms to the standard contract and assessment.

What interviewers listen for

- Watches for changing terms, not just initial assessment
- Connects to privacy obligations
- Updates standards for next time

The business owner will not act on vendor findings

You send findings to a vendor's business owner, who replies that risk is 'your job'. Findings sit open for months.

Situation read: Third-party risk fails when the business owner does not own the relationship.

What I'd do first: Clarify roles in policy, meet the owner to agree two priority actions, and include open findings in their management reporting.

Trade-offs: Escalating may sour the relationship; letting it slide normalises it.

What I'd tell leadership: I would report overdue findings by business owner to the risk committee so accountability sits with the relationship owner.

What interviewers listen for

- Clarifies first- and second-line roles
- Uses reporting to drive accountability
- Prioritises a few actions

Is a critical open-source library a supplier

Engineering relies on an open-source library maintained by one volunteer. Leadership asks whether TPRM covers it.

Situation read: There is no contract or questionnaire, yet it is a dependency with real risk.

What I'd do first: Work with engineering to inventory critical open-source components and track maintainer health, known vulnerabilities and update cadence.

Trade-offs: Forcing open source into vendor processes adds bureaucracy; ignoring it leaves a blind spot.

What I'd tell leadership: I would propose a joint ownership model: engineering owns the inventory and patching, TPRM sets criteria and reports concentration.

What interviewers listen for

- Expands third-party thinking appropriately
- Partners with engineering
- Keeps the process proportionate

Exit plans that exist only on paper

A regulator review asks you to evidence that exit plans for critical suppliers would work. The plans are templates nobody has tested.

Situation read: An untested exit plan is an assumption; the regulator wants evidence of feasibility.

What I'd do first: Pick the most critical supplier, run a tabletop exit with IT, procurement and the business owner, and record the time, cost and data-migration blockers found.

Trade-offs: Real testing takes effort from busy teams; a paper refresh is quick but will not satisfy the review.

What I'd tell leadership: I would report the gaps the test revealed, the remediation plan, and a schedule to test the remaining critical exits.

What interviewers listen for

- Tests rather than documents
- Involves the business owner
- Turns findings into a schedule