

GRC Interview & Study Guide

Third-Party & Vendor Risk

Prepared by **Naresh Thalla Mudhiraj** · thallanaresh.com

Personal learning project. Views are my own and do not represent any employer.

Basic to Advanced · scenario-based questions · practical examples · why each topic matters

Version 2.0 · generated 21 October 2026

Assessing and monitoring suppliers, cloud providers and the wider supply chain.

Study material written in plain language. Framework and regulatory details change; always confirm against the official, current publication before relying on them.

Third-Party & Vendor Risk

Assessing and monitoring suppliers, cloud providers and the wider supply chain.

Q: What is third-party risk management (TPRM) and why is it important?

Basic

TPRM is the process of identifying, assessing, mitigating and monitoring risks arising from vendors, suppliers, service providers, partners and their own subcontractors (fourth parties).

- Organisations increasingly outsource critical processes and data to third parties (cloud, SaaS, billing, support).
- You can outsource the service but not the accountability — regulators and customers hold you responsible.
- Many major breaches have originated in the supply chain.

Practical example: A billing vendor with remote access to a hospital's network is compromised, and attackers pivot into the hospital. TPRM would have required MFA, least-privilege access and contract notification terms before onboarding.

Why this matters: Vendor risk is a top concern for regulators and boards, and is explicitly addressed by ISO 27001, NIST CSF 2.0 (Govern), HIPAA (BAAs), GDPR (processors) and national regulations.

Q: What are standard vendor security questionnaires?

Basic

Instead of custom questionnaires, many organisations use industry standards:

- Shared Assessments SIG (Standardized Information Gathering) questionnaire.
- Cloud Security Alliance CAIQ (Consensus Assessments Initiative Questionnaire), aligned to the Cloud Controls Matrix.
- Sector-specific options exist, e.g. in healthcare.

Questionnaires should be validated with evidence (reports, policies, test results) for higher-risk vendors — self-attestation alone is weak assurance.

Practical example: Instead of a custom 400-question form, you accept the vendor's completed SIG Lite or CAIQ (cloud), plus their ISO 27001 certificate and SOC 2, and ask only follow-up questions where there are gaps.

Why this matters: Standard questionnaires save time for both sides and make vendor comparisons more consistent.

Q: What is the difference between a third party, a vendor, a supplier and a fourth party?

Basic

- **Third party:** any external organisation the company has a relationship with, including vendors, suppliers, partners, contractors, resellers and outsourcers.
- **Vendor or supplier:** a third party that provides goods or services. In practice the terms are often used interchangeably.
- **Fourth party:** your vendor's vendors (subcontractors and sub-processors), such as the cloud provider hosting your SaaS vendor.
- **Nth party:** further down the chain.

Practical example: A hospital's TPRM inventory covers software vendors but not visiting locum agencies or the medical device maintenance firm with remote access. Both are added after a review shows they handle patient data.

Why this matters: Defining the population clearly decides what your TPRM programme covers. Many programmes miss partners and contractors who are not formally 'vendors'.

Q: What is inherent versus residual vendor risk?

Basic

- **Inherent vendor risk:** the risk the relationship carries before considering the vendor's controls. It is based on data access, system access, criticality of the service, regulatory impact and spend.
- **Residual vendor risk:** what remains after assessing the vendor's controls and any extra controls you add (contract terms, restricted access, monitoring).
- Inherent risk decides the tier and depth of assessment. Residual risk decides approval, conditions and how often you review.

Practical example: A cloud EHR vendor has high inherent risk (patient data, critical service). After reviewing its SOC 2, ISO certificate and contract terms, residual risk is rated medium and it is approved with annual reassessment.

Why this matters: Separating the two avoids wasting effort on low-risk vendors while making sure high-risk ones get proper scrutiny.

Q: What is due diligence in vendor onboarding?

Basic

Due diligence is the set of checks done before signing with a vendor, proportionate to its risk:

- **Security and privacy:** questionnaires, certifications (ISO 27001, SOC 2), penetration test summaries, policies.
- **Financial stability and ownership:** can they stay in business, and are there sanctions or conflicts?
- **Legal and compliance:** data location, sub-processors, regulatory licences, litigation history.
- **Operational resilience:** BCP/DR, support model and SLAs.
- Reputation and ESG concerns where relevant.

Practical example: During due diligence for a new payroll provider, the team finds that data is processed in a country not covered by its transfer arrangements. The contract is changed to keep processing in approved locations before signing.

Why this matters: Problems found before signing are cheap to fix. After signing, your leverage drops sharply.

Q: Describe the third-party risk management lifecycle.

Intermediate

1. **Planning and sourcing:** define the business need and data/system access involved.
2. **Inherent risk scoring / tiering:** classify the vendor by criticality and data sensitivity.
3. **Due diligence:** questionnaires, SOC 2 / ISO 27001 reports, policies, pen test summaries, financial and reputational checks — depth based on tier.
4. **Risk assessment and remediation:** identify gaps, agree remediation or compensating controls, or decide not to proceed.
5. **Contracting:** security, privacy, audit rights, breach notification, subcontracting and exit clauses.

6. **Ongoing monitoring:** periodic reassessment, security ratings, news monitoring, performance and incident tracking.
7. **Offboarding:** revoke access, return or destroy data, obtain confirmation.

Practical example: Onboarding a cloud call-centre: plan and scope → inherent risk tiering → due diligence (SOC 2, questionnaire) → contract clauses → ongoing monitoring (annual reassessment, security ratings) → offboarding (data return and access removal).

Why this matters: A lifecycle approach avoids the common trap of assessing a vendor once at onboarding and never again.

Q: How do you tier vendors?

Intermediate

Vendor tiering assigns an inherent risk level so assessment effort matches risk. Common factors:

- Type and volume of data accessed (e.g. PHI, personal data, card data, confidential IP).
- Level of system or network access.
- Criticality of the service to operations (what if it fails for a week?).
- Regulatory relevance and geography (e.g. data hosted outside the country).
- Substitutability and concentration (how hard is it to replace?).

High-tier vendors get full due diligence and annual reviews; low-tier vendors may only need a short questionnaire.

Practical example: Tier 1: an EHR hosting vendor (patient data, critical service). Tier 2: an HR SaaS with employee PII. Tier 3: a catering supplier with no data or system access. Assessment depth follows the tier.

Why this matters: Tiering lets a small GRC team focus on the vendors that could really hurt the organisation.

Q: What security clauses should be in a vendor contract?

Intermediate

- Security requirements and adherence to standards/policies.
- Data protection terms (e.g. BAA under HIPAA, data processing agreement under GDPR/DPDP), including data location and transfer restrictions.
- Breach and incident notification obligations with defined timeframes.
- Right to audit or to receive independent assurance reports (SOC 2, ISO 27001 certificate).
- Subcontractor (fourth-party) approval and flow-down obligations.
- Business continuity and service level commitments.
- Data return and secure destruction at termination; exit and transition support.
- Liability, indemnity and insurance requirements.

Practical example: A contract for a cloud data processor includes: breach notification within 24–72 hours, right to audit or accept a SOC 2, data location limits, sub-processor approval, encryption requirements and data deletion on exit.

Why this matters: If it isn't in the contract, you usually cannot enforce it later — especially during an incident.

Q: How does the cloud shared responsibility model affect risk management?

Intermediate

In cloud services, security responsibilities are split between the provider and the customer, and the split depends on the model:

- **IaaS:** provider secures physical infrastructure and virtualisation; customer secures operating systems, applications, data, identities and configuration.
- **PaaS:** provider also manages the platform/runtime; customer manages applications, data and access.
- **SaaS:** provider manages most of the stack; customer is still responsible for data, user access, configuration and use.

Common failures come from customers assuming the provider handles something it does not, such as misconfigured storage or excessive permissions.

Practical example: In IaaS the provider secures the hypervisor and data centre. The customer must still configure security groups, patch VMs and manage IAM. Most cloud breaches come from the customer's side of the line.

Why this matters: Misunderstanding the shared responsibility model is one of the most frequent root causes of cloud data exposure.

Q: A critical vendor fails your security assessment, but the business insists on using them. What do you do?

Intermediate · Scenario

- Clarify the specific gaps and translate them into business risk (data exposure, regulatory impact, operational impact).
- Work with the vendor on a remediation plan with dates, and include it in the contract.
- Identify compensating controls on your side (e.g. limit data shared, encryption, extra monitoring, SSO with MFA).
- If residual risk remains above appetite, document it and route it for formal risk acceptance by an appropriate authority.
- Set conditions and reassessment dates; track remediation through to closure.

Practical example: A marketing analytics vendor lacks SSO and encryption at rest. The business needs it for a launch. Approve with conditions: no PHI uploaded, contract commitment to fix in 90 days, a VP-signed risk acceptance, and reassessment at day 90.

Why this matters: This shows you can enable the business while keeping risk visible and owned — the essence of GRC.

Q: How do you use security ratings services and continuous monitoring in TPRM?

Intermediate

- Security ratings tools scan a vendor's internet-facing footprint (exposed services, patching, email security, leaked credentials) and give a score.
- Useful for monitoring many vendors between assessments and for spotting sudden changes.
- **Limitations:** they only see the outside, can misattribute assets and do not reflect internal controls.
- Combine them with threat and news monitoring (breaches, financial distress) and with periodic assessments.
- **Define triggers:** a big score drop or a reported breach starts a vendor follow-up.

Practical example: A Tier 1 vendor's rating drops after an exposed remote desktop service appears on its network. The TPRM team contacts the vendor within 24 hours, and the service is closed within two days.

Why this matters: Annual questionnaires are a snapshot. Continuous signals help you react between reviews, but they should not replace evidence-based assessment.

Q: What should a vendor offboarding (exit) process include?

Intermediate

- **Revoke all access:** accounts, VPN, API keys, shared credentials and physical badges.
- Recover or securely delete data, with a certificate of destruction or evidence of return.
- Transition services and knowledge if replacing the vendor.
- Close or update contracts, and check surviving obligations such as confidentiality.
- Update the vendor inventory, risk register and data flows.
- For critical vendors, have an exit plan prepared in advance (a DORA requirement for EU financial entities, and good practice everywhere).

Practical example: When a hospital ends a contract with a transcription service, it disables the vendor's SFTP account and API keys, receives a deletion certificate for 3 years of audio files, and removes the vendor from its RoPA.

Why this matters: Offboarding is often forgotten. Former vendors with live access or retained data are a real breach source.

Q: How do you assess a SaaS vendor's security efficiently?

Intermediate

- **Start with the data and integration:** what data goes in, how users authenticate (SSO), and what integrations or API scopes are needed.
- **Request existing assurance first:** SOC 2 Type II, ISO 27001 certificate and SoA, penetration test summary, a trust centre.
- **Focus on key controls:** encryption, access management (SSO, MFA, RBAC), logging, vulnerability management, incident notification, data location and deletion, sub-processors.
- **Check the configuration you control:** tenant settings, admin roles, audit logs.
- Ask follow-up questions only where evidence is missing.

Practical example: For a new collaboration SaaS, the team reviews its SOC 2, confirms SSO and data residency options, enables audit logging and restricts external sharing in the tenant. The review takes 5 days instead of 5 weeks.

Why this matters: Efficient SaaS reviews keep up with the speed of business adoption without lowering standards.

Q: A vendor tells you they had a security incident but cannot share details yet. What do you do?

Intermediate · Scenario

1. Log it as a potential incident and inform your incident response team and privacy/legal.
2. **Ask the key questions in writing:** what services and data are affected, is your data involved, what is the timeline, what containment is in place, and when will they update you?
3. **Check your contract:** notification timelines, cooperation duties and audit rights.
4. **Take protective steps:** rotate shared credentials or API keys, review logs for activity from the vendor's connections, and consider suspending integrations.
5. Track your own regulatory clocks. Your notification duty may start when you become aware, not when the vendor finishes its investigation.
6. Follow up until closure and reassess the vendor afterwards.

Practical example: A file-transfer vendor reports 'suspicious activity'. The hospital disables the integration, rotates the SFTP credentials and checks logs. Two days later the vendor confirms the hospital's data was not affected, and the decision log records each step.

Why this matters: Vendor incidents are often reported slowly and vaguely. Acting on your own side immediately limits harm and protects your compliance position.

Q: Procurement signed a contract with a new vendor without a security review. What do you do?

Intermediate · Scenario

- **Assess the vendor now, prioritising by its inherent risk:** what data and access does it already have?
- If high risk, apply interim controls (restrict data and access) until the review is done.
- Check whether the contract has security clauses. If not, negotiate an addendum or data processing agreement.
- **Fix the process:** build the security review into the procurement workflow (no purchase order for in-scope categories without a TPRM ticket), and train procurement.
- Report the process gap as a finding if it is a pattern.

Practical example: A department bought a survey tool that collects patient feedback with names. The review finds no DPA, so one is signed within a week, and procurement adds a mandatory 'data involved?' question that routes purchases to TPRM.

Why this matters: Bypassed reviews are a process failure, not just a one-off. Fixing the workflow prevents repeats.

Q: The business wants to give a vendor's support team permanent admin access to a production system. What controls do you require?

Intermediate · Scenario

- **Challenge the need:** can access be time-bound and approved per session instead of permanent?
- Require named accounts (no shared logins), MFA and access through a controlled path such as a privileged access management tool or jump host.
- **Least privilege:** only the systems and rights needed.
- Session logging or recording, with review of high-risk activity.
- **Contract terms:** confidentiality, background checks, incident notification and liability.
- Periodic access reviews and immediate removal when staff change.

Practical example: The imaging system vendor gets just-in-time access through the PAM tool. Each session needs approval from the hospital IT on-call engineer, is recorded, and expires after 4 hours.

Why this matters: Vendor remote access is one of the most common breach routes. Strong controls let the vendor do its job without creating a permanent back door.

Q: A vendor's SOC 2 report shows exceptions in access reviews. How do you decide whether this matters to you?

Intermediate · Scenario

- **Read the exception details:** how many samples failed, what kind of access, and over what period.
- Check whether the failing control affects the services and data you use.
- Look at management's response and remediation date.

- Check for compensating controls in the report or in your own environment (for example, your own SSO and access reviews on the vendor platform).
- **Decide:** accept with follow-up, require remediation evidence, or escalate if the risk is significant. Record the decision in the vendor file.

Practical example: Two of 25 terminated vendor employees kept access for a week. The vendor has since automated deprovisioning. Because your data sits in an encrypted tenant you administer, you accept the finding and ask for evidence of the fix at the next review.

Why this matters: Exceptions are information, not an automatic fail. Good TPRM interprets them in the context of your own risk.

Q: What is fourth-party and concentration risk?

Advanced

- **Fourth-party risk:** risk from your vendors' own suppliers (e.g. your SaaS provider's hosting provider). You usually have no direct contract with them, so you rely on your vendor's controls, contractual flow-downs and SOC reports listing subservice organisations.
- **Concentration risk:** dependence on a single provider (or a few) for many critical services, so one failure has a wide impact — e.g. many services hosted with the same cloud provider or region.

Mitigations include mapping critical supply chains, requiring disclosure of material subcontractors, multi-region or multi-provider designs where justified, and exit planning.

Practical example: Five of your critical SaaS vendors all run on the same cloud region and use the same identity provider. A single outage there would hit all five at once. That is concentration and fourth-party risk.

Why this matters: Recent large-scale outages and supply chain attacks have made these topics a board-level concern.

Q: How do you manage software supply chain risk (open source, SBOMs, vendor updates)?

Advanced

- Inventory software components, ideally through Software Bills of Materials (SBOMs) from vendors and your own builds.
- Monitor components for vulnerabilities and use frameworks such as NIST SSDF (SP 800-218) for secure development expectations.
- Require vendors to have secure development practices, signed updates and timely vulnerability disclosure.
- Protect your build pipeline (access control, integrity checks, dependency pinning).
- Include software supply chain events in incident playbooks, such as a compromised update or a critical library vulnerability.

Practical example: When a critical vulnerability is announced in a common logging library, a company with SBOMs identifies affected applications in hours and asks the three vendors listed as using it for their patch status.

Why this matters: Attacks through trusted software updates and widely used open-source libraries have shown that supply chain risk can affect thousands of organisations at once.

Q: How do you measure and report the health of a TPRM programme?

Advanced

- **Coverage:** percentage of vendors inventoried and tiered; percentage of Tier 1 and 2 vendors assessed on time.
- **Risk:** number of vendors with high residual risk, open vendor issues by age, and vendors with expired assurance (old SOC 2 reports).
- **Contract:** percentage of critical vendors with required security clauses and exit plans.
- **Events:** vendor incidents, response times and notification compliance.
- **Concentration:** critical services dependent on a single provider.

Report to the risk committee with trends and the few vendors that need decisions.

Practical example: The quarterly report shows 96% of Tier 1 vendors assessed on time, 4 vendors with expired SOC 2 reports, and 3 critical services all relying on one cloud region. The last point leads to a resilience review.

Why this matters: Metrics show whether the programme reduces risk or only produces questionnaires.

Q: Your most critical cloud provider has a region-wide outage. What should TPRM and BCM have prepared?

Advanced · Scenario

- **Concentration analysis:** know which services depend on that provider and region, including fourth parties (SaaS vendors hosted there).
- **Architecture:** multi-zone or multi-region designs for critical services, with tested failover.
- **Exit and contingency plans:** documented and tested, including manual workarounds.
- **Contracts:** SLAs, credits, status communication and support escalation paths.
- **Communication:** templates for customers and regulators about service disruption.
- **After the event:** review actual impact against the BIA and adjust the strategy.

Practical example: During a regional outage, the patient portal fails over to a second region in 40 minutes as tested. But a SaaS scheduling vendor hosted in the same region is down for 6 hours, so clinics use paper downtime procedures, and the vendor's resilience becomes a contract renewal topic.

Why this matters: Cloud concentration is now a board-level and regulator topic. Preparation is the difference between a short disruption and a crisis.

Q: A Tier 1 vendor refuses to complete your questionnaire, saying 'we are too big to fill in customer forms'. How do you handle it?

Advanced · Scenario

- Accept that large providers often will not complete custom questionnaires, but still need assurance.
- **Use what they publish:** SOC 2 Type II, ISO 27001/27017/27018 certificates, CSA STAR entries, trust centre documentation and contractual commitments.
- Map that evidence to your requirements and note gaps.
- **Focus on your side of shared responsibility:** configuration, identity, logging and encryption choices.
- Where gaps remain, record residual risk and get it accepted by the business owner.

Practical example: A hyperscale cloud provider declines the questionnaire. The team maps its SOC 2 and ISO certificates to 85% of requirements, documents the customer-side controls for the rest, and the CIO signs off the residual risk.

Why this matters: TPRM must be practical. The goal is enough assurance to make an informed decision, not a completed form.

Q: You need to assess 300 existing vendors with a team of two. How do you plan it?

Advanced · Scenario

1. Build the inventory with spend data from finance, SSO and network data, and contract lists.
2. Tier every vendor with a short inherent-risk questionnaire completed by the business owner.
3. Focus deep assessments on Tier 1 (maybe 20–30 vendors) and lighter, evidence-based reviews on Tier 2.
4. For Tier 3, rely on contract terms and periodic attestation only.
5. Reuse existing assurance (SOC 2, ISO) and shared assessment services where possible.
6. **Automate with a TPRM tool:** reminders, questionnaires and scoring.
7. Agree a phased schedule with leadership and report progress.

Practical example: Tiering reduces the 300 vendors to 24 Tier 1, 70 Tier 2 and 206 Tier 3. The two-person team completes all Tier 1 assessments in the first quarter and shows the risk committee a clear plan for the rest.

Why this matters: Risk-based tiering is the only way to cover a large population with limited resources, and it is what regulators and auditors expect to see.