

GRC Interview & Study Guide

Scenario & Behavioural

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

Situational and behavioural questions. Use the STAR method (Situation, Task, Action, Result) and tailor the examples to your own experience.

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

Scenario & Behavioural

Situational and behavioural questions. Use the STAR method (Situation, Task, Action, Result) and tailor the examples to your own experience.

Q: Tell me about yourself (GRC version).

Basic

Structure a 60–90 second answer: present → past → future.

- **Present:** your current role, scope and environment (e.g. cyber risk governance in a healthcare technology company; frameworks such as ISO 27001, NIST, SOC 2, HIPAA).
- **Past:** 2–3 achievements with measurable outcomes (e.g. led a certification, built a risk register, reduced overdue findings, improved vendor assessment turnaround).
- **Future:** why this role — e.g. bringing regulated-industry GRC experience to a growing team and learning new frameworks.

Keep it relevant to the job description; avoid reciting your CV line by line.

Practical example: 'I'm a CISA-certified ISO 27001 Lead Auditor working in cyber risk governance for a healthcare technology company. I run risk assessments, audits and vendor reviews across ISO 27001, SOC 2 and HIPAA, and I want to bring that to regulated healthcare and financial services at a larger scale.'

Why this matters: First impressions shape the whole interview. A crisp, outcome-focused story sets the tone.

Q: Why do you want to work in GRC?

Basic

Tailor this to your own motivation. Good themes:

- Rapid digital transformation and a strong focus on cyber security and data protection, creating demand for experienced GRC professionals.
- The chance to apply framework experience (ISO 27001, NIST, SOC 2, HIPAA) while learning new regulations relevant to the employer.
- Interest in a specific sector, e.g. healthcare, government or financial services.
- Long-term commitment to the field and the role.

Avoid answers focused only on salary or job title.

Practical example: 'Organisations are investing heavily in digital health and regulation is catching up fast. My mix of healthcare, ISO 27001 and audit experience fits that growth directly.'

Why this matters: Employers want candidates who are motivated by the work and committed to staying.

Q: How do you use the STAR method to answer behavioural questions in a GRC interview?

Basic · Scenario

STAR stands for Situation, Task, Action, Result:

- **Situation:** brief context, such as the organisation, team, and what was happening.
- **Task:** your responsibility or the goal.
- **Action:** what you did, specifically. Use 'I', not just 'we'. This should be the longest part.
- **Result:** the outcome, with numbers if possible, and what you learned.

Prepare 6–8 stories in advance that cover common themes: audit, risk, conflict, failure, influence, deadlines, learning.

Practical example: Situation: an ISO 27001 surveillance audit was 6 weeks away with 14 open actions. Task: I owned audit readiness. Action: I prioritised by risk, ran weekly owner check-ins and built an evidence tracker. Result: 12 were closed before the audit, the audit had no major nonconformities, and the tracker is now standard.

Why this matters: Behavioural questions decide many GRC interviews. A structured answer shows clear thinking and real experience.

Q: Tell me about a time you made a mistake at work. What happened?

Basic · Scenario

- Choose a real but manageable mistake, not a disaster and not a fake 'weakness'.
- Explain the situation briefly and take ownership. Do not blame others.
- Focus on how you noticed it, what you did to fix it and who you told.
- End with what you changed so it would not happen again (process, checklist, habit).

Interviewers want honesty, accountability and learning.

Practical example: 'I sent a draft audit report with an incorrect sample count to a control owner. I noticed within an hour, told them and my manager, corrected it, and added a peer-review step before any finding leaves the team. We have not had a similar error since.'

Why this matters: In GRC, integrity and transparency matter most. This question tests whether you report problems or hide them.

Q: Why should we hire you for a GRC role in healthcare?

Basic · Scenario

- **Connect your experience directly to their needs:** regulated healthcare data, audit and certification, risk governance and vendor risk.
- Mention your credentials briefly (for example CISA and ISO 27001 Lead Auditor) and what you have done with them.
- **Show awareness of the rules that apply to them:** the local data protection law, health regulator requirements and data localisation.
- Give one or two short results with numbers.
- End with enthusiasm for their mission.

Practical example: 'In my last role I cut supplier assessment turnaround from six weeks to ten days and took the company through its first ISO 27001 surveillance audit with no major nonconformities. You are scaling up supplier onboarding and preparing for certification, which is exactly that work.'

Why this matters: This closing question is your summary pitch. A focused, evidence-based answer is far more convincing than general statements.

Q: You join an organisation with no formal GRC programme. What do you do in your first 90 days?

Intermediate · Scenario

- **Days 1–30 (understand):** meet stakeholders, learn business objectives, regulatory and contractual obligations, existing policies, past audits and incidents; identify crown-jewel assets and key vendors.
- **Days 31–60 (assess):** run a high-level gap assessment against a chosen framework (e.g. ISO 27001 or NIST CSF 2.0), stand up an initial risk register with the top risks and owners, and agree a risk methodology.

- **Days 61–90 (plan):** propose governance (committee, policy framework, RACI), a prioritised roadmap with quick wins, metrics and resource needs; get leadership sign-off.

Throughout: build relationships and deliver a few visible quick wins (e.g. MFA gaps, an exception process).

Practical example: Days 1–30: meet stakeholders, inventory obligations and current controls. Days 31–60: run a high-level risk assessment, draft the policy framework and set up a risk register. Days 61–90: present a prioritised roadmap and governance structure to leadership for approval.

Why this matters: This tests strategic thinking, prioritisation and stakeholder management — not just framework knowledge.

Q: How do you explain a technical risk to a non-technical executive?

Intermediate · Scenario

- **Start with the business impact:** 'If this happens, we could be unable to process customer orders for several days and may have to notify regulators.'
- Explain likelihood simply and honestly, with evidence (e.g. similar incidents in the sector, exposure findings).
- Avoid jargon; use analogies if helpful.
- Present options with cost, effort and risk reduction, and a recommendation.
- Be clear about the decision you need and by when.

Practical example: Instead of 'TLS 1.0 is enabled on the patient portal', say 'Our patient portal uses an outdated security setting that regulators and some customers treat as non-compliant. Fixing it takes two days and removes the risk of failing next month's audit.'

Why this matters: GRC is largely about influencing decisions. Executives act on business impact, not CVE numbers.

Q: Tell me about a time you had to push back on a stakeholder.

Intermediate · Scenario

Use STAR. A strong example covers:

- **Situation/Task:** e.g. a business leader wanted to launch a system or onboard a vendor that had unresolved high risks.
- **Action:** you listened to their goals, quantified or clearly described the risk, proposed alternatives (phased launch, compensating controls) and, where needed, used the formal risk acceptance/escalation route.
- **Result:** a decision was made with the risk understood and documented; ideally the project still delivered with reduced risk, and the relationship stayed positive.

Emphasise collaboration and process rather than 'winning' the argument.

Practical example: A product head wanted to launch without a penetration test. You showed the customer contract required one, proposed a focused 5-day test instead of a full one, and the launch slipped only a week with the risk documented.

Why this matters: Interviewers look for assertiveness balanced with business empathy and professionalism.

Q: You have 40 open audit findings and limited resources. How do you prioritise?

Intermediate · Scenario

- Rate each finding by risk (impact and likelihood), regulatory or contractual exposure, and whether it is a repeat finding.

- Group findings by root cause — fixing one systemic issue (e.g. no joiner-mover-leaver process) may close several findings.
- Identify quick wins that reduce risk with little effort.
- Agree a realistic plan with owners and dates; get leadership support for the high-risk items.
- Communicate transparently with auditors about the plan and track progress through governance.

Practical example: Of 40 findings, 11 trace back to applications with no named owner in the CMDB, so nobody reviews their access, patching or backups. Assigning owners with the business units closes the root cause of all 11, so it goes to the top of the plan, along with 3 high-risk regulatory items.

Why this matters: Prioritisation under constraints is the daily reality of GRC work.

Q: A new regulation is announced that affects your organisation. How do you respond?

Intermediate · Scenario

1. Read the official text and guidance; confirm applicability and effective dates (involve legal).
2. Break it into specific requirements and map them to existing controls and policies.
3. Identify gaps and estimate effort and cost.
4. Assign owners and build a compliance roadmap with milestones before the effective date.
5. Brief leadership on impact, risk of non-compliance and resource needs.
6. Implement, collect evidence and monitor for further guidance or amendments.

Practical example: When a new national privacy law came in, a GRC lead ran an applicability assessment, a gap analysis against existing GDPR controls, assigned owners for the gaps, and briefed the executive committee on timelines and budget.

Why this matters: Regulatory change management is a core GRC responsibility — especially in fast-evolving markets.

Q: A control owner is defensive and refuses to accept an audit finding. How do you handle it?

Intermediate · Scenario

- Stay calm and focus on facts. Walk through the criteria, the evidence and the condition together.
- Listen. They may have evidence you have not seen, or the finding may be worded unfairly.
- If you are wrong, correct the finding. If you are right, explain the risk in their terms and how it affects them.
- Work on the remediation together and agree realistic dates.
- If disagreement continues, record management's response and escalate through the agreed audit process.

Practical example: The owner argued that the backups were tested. Their evidence showed backup job success, not restore tests. After seeing the policy requirement, they agreed, and a quarterly restore test was added within a month.

Why this matters: Auditors and GRC professionals need people's cooperation. Handling disagreement professionally keeps relationships and findings intact.

Q: You are given a GRC task in an area you know little about, such as OT security. What do you do?

Intermediate · Scenario

- Acknowledge the gap honestly to your manager and set realistic expectations.

- **Learn the basics quickly:** key standards (for OT, IEC 62443 and NIST SP 800-82), the main risks and terminology.
- Find internal experts and involve them early. Engineers know their systems better than you do.
- **Apply your transferable GRC skills:** risk assessment, control frameworks, interviews and evidence.
- Validate your conclusions with subject matter experts before reporting.

Practical example: Asked to assess risk at a hospital's building management system, I read the NIST OT security guide, interviewed the facilities engineer and found that the system was reachable from the corporate network. Segmentation was added within a month.

Why this matters: Nobody knows every domain. Interviewers want to see how you learn and how you combine GRC methods with expert knowledge.

Q: Your manager asks you to finish a risk assessment in 2 days instead of 2 weeks. What do you do?

Intermediate · Scenario

- **Clarify why:** is there a deadline such as a board meeting or a go-live?
- **Propose a reduced scope:** focus on the highest-risk areas, use existing evidence (SOC 2, previous assessments) and hold one workshop with key people.
- Be clear about limitations in the output ('rapid assessment, based on X, not including Y').
- Agree a follow-up to complete the full assessment later if needed.
- Deliver on time with transparent assumptions.

Practical example: I delivered a 4-page rapid assessment in 2 days, covering the 6 highest risks with clear assumptions. The go-live was approved with two conditions, and a full assessment followed within the month.

Why this matters: Speed and quality are always in tension. Interviewers want to see you can deliver useful results quickly without hiding limitations.

Q: A business leader says 'security is slowing us down'. How do you respond?

Intermediate · Scenario

- **Listen first and get specifics:** which process, which delay, what impact?
- **Often the problem is fixable:** unclear requirements, slow approvals or a missing self-service option.
- **Offer solutions:** pre-approved patterns, risk-based fast tracks for low-risk changes, clear timelines for reviews.
- Explain the risks of skipping controls in their terms, without lecturing.
- Measure and share improvements, such as review turnaround time.

Practical example: Vendor reviews took 6 weeks. I introduced a tiering questionnaire so low-risk tools are approved in 2 days, and the average time fell to 9 days while high-risk vendors still received full reviews.

Why this matters: GRC teams that are seen as blockers lose influence. Making security easy to follow is part of the job.

Q: You are the only GRC person in a growing company. How do you prioritise your work?

Intermediate · Scenario

- **Understand the business priorities:** customers and contracts that need certifications, upcoming audits, regulatory deadlines.

- Address the highest risks and must-haves first, such as MFA, backups, access reviews and incident response basics.
- **Build lightweight foundations:** a risk register, a policy set and an obligations register.
- Use automation and existing tools rather than building heavy processes.
- Report simply to leadership and agree priorities, so trade-offs are their decisions.
- Build champions in each team to extend your reach.

Practical example: As the first GRC hire, I focused the first quarter on SOC 2 readiness because it blocked two enterprise deals. I set up a risk register and recruited 6 security champions across engineering and operations.

Why this matters: A one-person GRC function must be ruthlessly risk-based. Interviewers want to see judgement and influence, not just knowledge.

Q: A ransomware attack hits a key system. What is your role as a GRC lead?

Advanced · Scenario

- Make sure the incident response plan is activated with the right people (IR, IT, legal, privacy, communications, leadership).
- **Support impact assessment:** which data and processes are affected, whether personal or health data may be involved.
- Track regulatory, contractual and insurer notification timelines (e.g. HIPAA, GDPR, national requirements, customer contracts) and support legal in decision-making.
- Keep a clear decision and evidence log.
- **Coordinate continuity:** check BCP and DR activation against RTO/RPO.
- **Afterwards:** lead lessons learned, update the risk register, track remediation and report to leadership and the board.

Decisions on ransom payment are for senior leadership with legal advice; GRC helps make sure they are informed and documented.

Practical example: While IT restores systems, the GRC lead runs the decision log, checks regulatory deadlines with legal, prepares board updates every 4 hours and later leads the post-incident control review.

Why this matters: This shows you understand the GRC role in a crisis and the regulatory consequences of incidents.

Q: How would you approach governance of AI use in the organisation?

Advanced · Scenario

- Inventory AI use cases, including third-party tools and features embedded in existing software.
- Classify use cases by risk (e.g. use of personal or health data, automated decisions affecting people, customer-facing outputs).
- Set an AI acceptable-use policy and approval process; involve privacy, legal, security and business owners.
- Assess risks such as data leakage, accuracy and bias, explainability, security of models and vendor terms.
- **Use recognised references:** ISO/IEC 42001 (AI management system), the NIST AI Risk Management Framework, and regulations relevant to your markets, such as the EU AI Act.
- Monitor, review and report AI risks through existing governance rather than creating a separate silo.

Practical example: A company forms an AI governance group, publishes an acceptable-use policy for generative AI tools, keeps an inventory of AI systems with risk ratings, and uses ISO/IEC 42001 and the NIST AI RMF as reference frameworks.

Why this matters: AI governance is a fast-growing GRC responsibility, and interviewers increasingly ask how you would handle it.

Q: You suspect a senior colleague is deliberately bypassing a control (for example approving their own changes). What do you do?

Advanced · Scenario

- **Gather facts quietly and carefully:** logs, tickets, approvals. Do not accuse anyone based on suspicion alone.
- Check whether there is a legitimate explanation, such as an emergency change process.
- **If the concern stands, report it through the right channel:** your manager, internal audit, compliance or the whistleblowing line, depending on seriousness and policy.
- Keep the matter confidential and avoid investigating beyond your role.
- Recommend a technical fix that prevents self-approval regardless of the person.

Practical example: Change logs showed a senior engineer approving 15 of his own production changes. It was reported to the head of IT and internal audit. It turned out to be a tooling gap, which was fixed by enforcing a two-person rule in the deployment pipeline.

Why this matters: Integrity issues involving senior people are delicate. Following the right channel protects you, the organisation and the person concerned.

Q: Your organisation is preparing for its first ISO 27001 certification in 6 months. Describe your plan.

Advanced · Scenario

1. **Month 1:** agree scope, get a sponsor, run a gap assessment and set the project plan.
2. **Months 1–2:** define the risk methodology, run the risk assessment, and draft the SoA and core policies.
3. **Months 2–4:** implement and evidence controls, run awareness, and start collecting operating evidence.
4. **Month 4:** run the internal audit across all clauses and key controls.
5. **Month 5:** hold the management review, fix findings, and run Stage 1.
6. **Month 6:** close Stage 1 observations, then Stage 2.

Throughout: keep leadership engaged and choose a certification body early, because their availability can drive the dates.

Practical example: Using this plan at a 150-person health-tech company, Stage 1 found 3 minor observations, all closed in 3 weeks, and Stage 2 resulted in certification with no major nonconformities.

Why this matters: This question tests whether you understand the full certification journey and can manage it as a project.

Q: The regulator announces an unannounced inspection tomorrow. What do you do today?

Advanced · Scenario

- Inform leadership, legal and the relevant owners immediately, and confirm who will host the inspectors.
- Confirm the scope and the inspector's likely focus if known.

- Prepare a room, a single point of contact, an attendance and request log, and a briefing for staff who may be interviewed (be honest, answer what is asked, do not guess).
- **Gather key documents:** policies, risk assessments, recent audit reports, incident logs and evidence of key controls.
- Do not create or change documents to make them look better. Present what exists.

Practical example: When the health regulator arrived, the hospital's GRC lead had a request log, a document index and a small team ready. All 22 requests were answered on the day, and the inspection closed with two minor observations.

Why this matters: Inspections test real readiness. Calm, honest coordination makes a much better impression than last-minute document creation.

Q: You discover your organisation has been reporting an incorrect compliance status to a customer for months. What do you do?

Advanced · Scenario

- **Confirm the facts quickly:** what was reported, what is the actual status, since when, and why.
- Inform your manager, legal and the account owner. Correcting it is not optional.
- Agree on a correction with legal, describing the actual status, impact and remediation plan.
- Fix the underlying control or gap and the reporting process (who approves customer statements and what evidence they rely on).
- Record it and learn from it. This is a trust issue as much as a compliance one.

Practical example: Quarterly reports to a hospital customer said 'all staff trained', but contractors had been excluded. The customer was informed with a correction and plan. Contractors completed training within 3 weeks, and statements now require GRC sign-off with evidence.

Why this matters: Customers base decisions on your assurance statements. Correcting errors promptly protects trust and reduces legal exposure.

Q: Where do you see GRC heading in the next five years, and how are you preparing?

Advanced · Scenario

- **Continuous assurance:** automated evidence and control monitoring replacing point-in-time audits.
- **AI governance:** ISO/IEC 42001, the EU AI Act and national AI policies creating new GRC responsibilities.
- **Quantified risk:** more financial expression of cyber risk for boards.
- **Regulatory growth and convergence:** privacy laws (GDPR, India DPDP), resilience rules (DORA, NIS2) and third-party oversight.
- **Preparation:** certifications and learning (for example AI governance), hands-on GRC automation skills, and building strong communication with business leaders.

Practical example: 'I'm studying ISO/IEC 42001 and the NIST AI RMF, I've automated evidence collection for access reviews using our GRC tool, and I follow EU and India regulatory updates so I can brief stakeholders early.'

Why this matters: Interviewers want people who keep learning and can help the organisation prepare for change, not just follow today's checklist.