

GRC Lead / Manager: senior interview pack

Running a GRC programme when priorities collide, evidence is messy and leadership wants a simple answer. Free from thallanaresh.com. Answers are outlines to adapt with your own examples.

Two certifications, one quarter, half a team

Sales has promised a prospect a new certification by quarter end. The same quarter holds your surveillance audit for the existing one, and two of your four analysts have resigned. The CRO asks whether you can do both.

Situation read: The real question is risk to revenue versus risk to an existing certificate. Losing the current certificate hurts more customers than one delayed deal.

What I'd do first: Map overlapping controls between the two frameworks, size the genuinely new work, and ask Sales for the exact contractual wording: is it 'certified' or 'in progress with a dated plan'?

Trade-offs: Contractors can draft evidence but cannot own controls. A readiness letter from the auditor may satisfy the prospect without a rushed audit.

What I'd tell leadership: I would protect the surveillance audit, offer the prospect a dated roadmap plus readiness assessment, and show the CRO the cost of backfilling versus slipping.

What interviewers listen for

- Separates what the customer actually needs from what was promised
- Uses control overlap instead of double work
- Gives leadership options with costs, not a yes or no

A policy everyone signs and nobody follows

Attestation for the clean-desk and data-classification policy is near 100%. A walk-through finds labels missing on most shared drives and sensitive files in open channels. The policy owner says 'the numbers are fine'.

Situation read: Attestation measures reading, not behaviour. The metric is green while the control outcome is red.

What I'd do first: Pull a small evidence sample (drives, channels, tickets) to quantify the gap, then sit with two teams to learn why the rule is ignored: friction, tooling or unclear labels.

Trade-offs: Rewriting the policy is cheap but changes nothing; tooling such as default labels costs more but moves behaviour. Naming teams publicly can backfire.

What I'd tell leadership: Retire attestation as the headline metric, report an outcome metric (labelled vs unlabelled sensitive locations) and propose one tooling fix with a 90-day target.

What interviewers listen for

- Distinguishes activity metrics from outcome metrics
- Looks for root cause before blame
- Changes what is reported upward

A director asks you to brief them privately

A non-executive director contacts you directly, outside the committee, asking for your 'honest view' of cyber risk because they distrust the CISO's reports.

Situation read: This may reveal a real reporting problem or a governance boundary being crossed; either way it is sensitive.

What I'd do first: Listen to what is driving the distrust, avoid giving an off-the-record view that contradicts formal reports, and tell the director you will raise the concern through the committee chair.

Trade-offs: Refusing may look evasive; briefing privately undermines your line management and the committee.

What I'd tell leadership: I would tell the CISO and chair that a director wants more depth, and propose a deep-dive session so the gap in confidence is fixed in the open.

What interviewers listen for

- Respects governance channels
- Treats distrust as a signal about reporting
- Stays transparent with their own leadership

Renew the GRC platform or hire an analyst

Budget allows either renewing an expensive GRC platform that is half-adopted or hiring one analyst. Finance wants your recommendation by Friday.

Situation read: The platform only has value if workflows run through it. Half adoption often means data is duplicated in spreadsheets anyway.

What I'd do first: Measure what actually runs in the tool today (assessments, issues, attestations), and price a downgrade tier or shorter term before choosing.

Trade-offs: Cutting the tool may break audit trails auditors rely on; skipping the hire overloads people already stretched.

What I'd tell leadership: I would present both options with what breaks under each, a negotiated cheaper renewal if possible, and the adoption milestones that justify keeping it.

What interviewers listen for

- Uses usage data, not opinion
- Thinks about audit trail and continuity
- Negotiates rather than accepts a binary

Teams send auditors evidence you have not seen

During an external audit, teams send evidence straight to the auditors. Some of it contradicts what GRC submitted, and the auditor asks which is right.

Situation read: Uncoordinated evidence creates inconsistency and possibly findings; it also signals the control narrative is not shared.

What I'd do first: Set up a single evidence channel immediately, reconcile the conflicting items with the owners, and give the auditor a corrected, explained set.

Trade-offs: Centralising slows things down; letting it continue risks contradictory findings.

What I'd tell leadership: I would explain the reconciliation to the auditor openly and agree an evidence protocol with owners for the rest of the audit.

What interviewers listen for

- Owns the audit relationship
- Reconciles before defending
- Sets clear protocols

Your regulator and your external auditor disagree

Your external auditor says a control design is acceptable. A regulator's examination letter calls the same control weak. Leadership asks which one to follow.

Situation read: They have different mandates; the regulator's view carries legal weight, but the auditor's reasoning may still be useful.

What I'd do first: Read the regulator's finding closely to understand the expectation, compare it with the auditor's testing scope, and identify the minimum design change that satisfies both.

Trade-offs: Pushing back on the regulator costs goodwill; over-engineering the control costs money.

What I'd tell leadership: I would recommend meeting the regulator's expectation with a proportionate fix, documenting why, and sharing the change with the auditor before year end.

What interviewers listen for

- Understands different assurance mandates
- Seeks a design that satisfies both
- Does not play one off against the other

A risk appetite statement nobody signed

You inherit a risk appetite statement drafted two years ago. It was never approved, yet teams cite it to justify accepting risks. An auditor is due next month.

Situation read: Risk acceptances made against an unapproved appetite have weak authority, and the auditor will notice.

What I'd do first: List the acceptances that cite the statement, rank them by exposure, and take a refreshed, shorter appetite statement to the committee for formal approval.

Trade-offs: Re-opening every acceptance is disruptive; leaving them hides a governance gap.

What I'd tell leadership: I would disclose the gap to the auditor myself with the remediation date, and ask leadership to re-confirm the highest-exposure acceptances under the approved statement.

What interviewers listen for

- Spots the authority problem behind the document
- Prefers self-disclosure to being found out
- Prioritises by exposure

The only person who runs a key control leaves

The single engineer who performed a quarterly key-rotation control leaves without handover. The next audit sample period has already started.

Situation read: This is a key-person dependency that turned into a control failure risk overnight.

What I'd do first: Find out when the control last ran, assign an interim owner, and write the procedure with them as they perform it for the first time.

Trade-offs: Rushing the first run risks mistakes; waiting risks a missed control instance the auditor will sample.

What I'd tell leadership: I would report the gap openly, the interim fix, and a rule that every key control has a named backup who has performed it at least once.

What interviewers listen for

- Spots key-person risk
- Documents while doing
- Builds resilience into ownership

Customer audit requests swamp the team

Your team receives dozens of customer security questionnaires and audit requests each month. Analysts spend more time answering them than improving controls.

Situation read: Customer assurance is revenue-critical but repetitive; the programme is being run by inbound demand.

What I'd do first: Analyse the requests for common questions, build a reusable answer library and a public trust pack, and set service levels with Sales.

Trade-offs: Self-service may not satisfy large customers; bespoke answers do not scale.

What I'd tell leadership: I would show leadership time spent, what the library saves, and propose that Sales owns first-pass answers with GRC reviewing exceptions.

What interviewers listen for

- Measures where team time goes
- Builds reusable assurance
- Rebalances ownership with Sales

Key risk indicators turn red and nothing happens

Your KRI dashboard has shown red on patch latency for three months. Nobody acts because 'it has always been red'.

Situation read: A threshold that never triggers action is not a threshold. Either the tolerance is wrong or the escalation path is missing.

What I'd do first: Confirm the data is accurate, then agree with the owner whether the threshold reflects real tolerance and what action red should trigger.

Trade-offs: Lowering the bar makes the dashboard green without reducing risk; holding it may need budget nobody has.

What I'd tell leadership: I would bring the KRI to the risk committee as a decision: fund the fix, formally accept the risk for a set period, or change the tolerance with a reason recorded.

What interviewers listen for

- Connects indicators to decisions
- Refuses to normalise permanent red
- Forces an explicit accept, fund or change choice