

IT Audit Manager: senior interview pack

Leading audits where evidence is thin, auditees push back and the committee wants clear opinions. Free from thallanaresh.com. Answers are outlines to adapt with your own examples.

A key report nobody can prove is complete

Your team relies on a system-generated user listing to test terminations. Midway through fieldwork, you learn the report was built by a contractor who left, and nobody can explain its query.

Situation read: If the report's completeness and accuracy are unproven, every test built on it is unreliable.

What I'd do first: Pause reliance, have the team reperform the extraction or reconcile record counts to the source tables, and document the steps as information provided by the entity testing.

Trade-offs: Re-running costs days of fieldwork; reporting with a caveat weakens the opinion.

What I'd tell leadership: I would tell the audit committee chair the timeline moved because the evidence base needed validation, which protects the opinion's credibility.

What interviewers listen for

- Knows completeness and accuracy testing of reports
- Stops before building on weak evidence
- Communicates delay as quality

The auditee rejects your high rating

You rate a finding on weak change approvals as high. The business head argues it should be low because 'nothing went wrong'. They plan to raise it with the CEO.

Situation read: Absence of an incident is not evidence a control works. The rating should follow your methodology, not the reaction.

What I'd do first: Re-check the facts and rating criteria with the team, then meet the business head to walk through impact and likelihood using the agreed scale.

Trade-offs: Downgrading keeps the relationship but erodes independence; holding firm without listening looks rigid.

What I'd tell leadership: I would keep the rating if the criteria support it, record management's view in the report, and brief the CAE before the CEO conversation happens.

What interviewers listen for

- Anchors ratings in methodology
- Lets management's response be recorded
- Escalates early to protect independence

An audit where you cannot see the system

You must audit a critical SaaS platform. The vendor refuses direct access and offers only its assurance report, which carves out a subservice provider.

Situation read: The assurance report covers part of the risk; the carve-out and your company's own configuration are untested.

What I'd do first: Map the report's controls to your audit objectives, list the complementary user entity controls, and test those plus your tenant configuration directly.

Trade-offs: Requesting a right-to-audit clause is slow; accepting the report alone leaves a gap.

What I'd tell leadership: I would report what was covered, what relied on third-party assurance, and the residual gap, and recommend the contract and vendor-management actions to close it.

What interviewers listen for

- Understands carve-outs and user entity controls
- Tests what is in the company's own control
- Is transparent about reliance

Your audit plan is cut mid-year

Budget cuts remove a third of your audit hours halfway through the year. The CFO suggests dropping the IT audits because they are 'technical'.

Situation read: Cutting by subject rather than risk could leave the highest exposures unaudited.

What I'd do first: Re-rank the remaining plan by risk, identify audits that could rely on second-line work, and show which risks lose coverage under each option.

Trade-offs: Relying on second line saves hours but needs you to assess their quality; deferring adds risk to next year's plan.

What I'd tell leadership: I would take a revised, risk-ranked plan to the audit committee for approval, making explicit which risks are uncovered by the cut.

What interviewers listen for

- Re-plans by risk, not convenience
- Makes coverage gaps visible to the committee
- Uses reliance carefully

A fraud signal turns up in an IT audit

While testing segregation of duties, your senior notices a user who created a vendor, approved its invoices and changed its bank details within a week.

Situation read: This may be fraud or a poorly designed workflow; either way, normal fieldwork could tip off a suspect.

What I'd do first: Preserve evidence, stop discussing it with the auditee, and escalate under the fraud protocol to the CAE and legal or investigations.

Trade-offs: Investigating yourself risks tainting evidence; waiting too long risks more loss.

What I'd tell leadership: I would brief the CAE immediately, keep the audit report factual about the SoD design gap, and let investigations handle the individual.

What interviewers listen for

- Knows when audit stops and investigation starts
- Protects evidence and confidentiality
- Separates control finding from individual conduct

Leadership wants continuous auditing next quarter

The audit committee chair saw a vendor demo and asks for continuous auditing across finance and IT next quarter. Your data access is patchy.

Situation read: Continuous auditing needs reliable data feeds and owners for exceptions; without them it produces noise.

What I'd do first: Pick one high-value, data-ready area such as privileged access or payments, prove the analytics, and define who triages exceptions.

Trade-offs: A broad launch impresses but floods teams; a narrow pilot looks slow but builds trust.

What I'd tell leadership: I would commit to a pilot with measurable exceptions found and closed, and a roadmap for wider coverage once data access is fixed.

What interviewers listen for

- Grounds hype in data readiness
- Defines exception ownership
- Commits to evidence of value

Last year's workpapers do not support last year's opinion

Preparing a follow-up, you find last year's workpapers for a satisfactory rating lack evidence for several key tests. The manager who signed has moved teams.

Situation read: This is a quality issue with your function's own work; it may affect reliance by external auditors.

What I'd do first: Assess whether the gaps change the conclusion by reperforming key tests now, and log it through the quality assurance process.

Trade-offs: Quiet re-testing protects reputation short term; formal disclosure is uncomfortable but defensible.

What I'd tell leadership: I would inform the CAE and, if the conclusion changes, the committee, and tighten review sign-off so it cannot recur.

What interviewers listen for

- Owns quality problems in their own function
- Reperforms before concluding
- Fixes the review process

Developers say change control blocks them

Engineering moved to many deployments a day. They say your change management testing is outdated and ask you to 'trust the pipeline'.

Situation read: The control objective is unchanged: only authorised, tested changes reach production. The evidence now lives in the pipeline.

What I'd do first: Walk through the pipeline with engineers to find the gates (peer review, automated tests, restricted deploy rights) and test those settings and their override logs.

Trade-offs: Testing pipeline configuration needs new skills; sampling tickets the old way misses bypasses.

What I'd tell leadership: I would explain to leadership that we audit the pipeline as the control, and report any bypass path as the key risk.

What interviewers listen for

- Keeps the objective while modernising the test
- Looks for override and bypass paths
- Builds credibility with engineers

Can you rely on management's self-assessment

The first line runs a control self-assessment that reports everything effective. The committee asks whether audit can use it to reduce testing.

Situation read: Self-assessments are useful but rarely independent; all-green results are a warning sign.

What I'd do first: Reperform a sample of their tests to measure accuracy before deciding any reliance.

Trade-offs: Reliance saves hours; misplaced reliance damages the audit opinion.

What I'd tell leadership: I would report the accuracy rate found and set reliance levels by area, with clear conditions for increasing it.

What interviewers listen for

- Tests before relying
- Treats uniform green as a red flag
- Sets graded reliance

The committee wants an opinion on cyber overall

The audit committee asks for an overall opinion on cybersecurity, but you have only audited a few areas this year.

Situation read: An overall opinion needs a basis; giving one from limited work overstates assurance.

What I'd do first: Combine your audits, second-line results and external assessments into an assurance map showing coverage and gaps by domain.

Trade-offs: A heat map is easy to read but can imply more certainty than exists.

What I'd tell leadership: I would give an opinion limited to the areas covered, show the assurance map, and propose the work needed for a full opinion next year.

What interviewers listen for

- Knows the limits of assurance
- Uses assurance mapping
- Plans to close coverage gaps