IT Auditor interview questions

careertips.com.au: common questions and what they're really testing

What to expect

IT auditor interviews usually blend technical control testing with scenarios and stakeholder communication. Employers want evidence you can plan an audit, test controls properly and explain risk to people who do not work in technology.

- **Process and methodology:** How you scope an audit, assess risk, design testing and document workpapers.
- **Technical control testing:** Access controls, change management, data integrity, IT general controls and the use of CAATs.
- **Compliance and frameworks:** ISO/IEC 27001, APRA CPS 234, the Essential Eight, Privacy Act obligations and reporting to regulators.
- **Behavioural:** Past findings, disagreements with management, tight deadlines and how you followed up remediation.
- **Scenario and judgement:** What you do when you find a serious control gap, when evidence is incomplete or when management pushes back.
- **Client-facing communication:** Explaining technical risk to finance managers, audit committees or boards.

Typically a screening call with a recruiter or hiring manager, then a technical interview with an audit manager or senior auditor covering methodology and control testing. After that comes a panel or stakeholder conversation with finance, risk or IT. Some employers include a short case study or a take-home review of a control description. Expect follow-up questions on how you document evidence and track findings to closure.

1. Walk me through how you plan and complete an IT audit, from scoping to final report.

Why they ask

This checks whether you understand audit methodology rather than just individual control tests.

How to structure your answer

Use a linear walk-through: context and objectives, risk assessment, scope and criteria, control testing, evidence and workpapers, findings and rating, management responses, reporting and follow-up.

Example answer

“I start by understanding the business process and the systems that support it, then I meet with the process owner and financial auditors to identify key risks. I map those risks to controls, for example access approval, segregation of duties, change management and backup restoration. I document the audit program and agree the scope with the audit manager. During fieldwork I test the controls using inquiry, observation, inspection and data analytics. For access controls I might pull user listings into ACL and compare them to approved role matrices. I keep workpapers that show the sample or full population, the criteria and the conclusion. When I find an exception I discuss it with the owner, draft a finding with a risk rating and a practical recommendation, and track the management response through to closure. The final report goes to the audit committee with a clear opinion and a status of agreed actions.”

2. Tell me about a time you identified a significant control weakness. How did you handle it?

Why they ask

This looks at professional scepticism, communication and whether you follow findings through to remediation.

How to structure your answer
Use STAR: situation, task, action, result. Keep the action section focused on how you confirmed the issue, escalated it and tracked the fix.

Example answer

“At a previous employer, I was testing change management over a financial reporting system. I found that several emergency changes had been deployed without retrospective approval, and the evidence of testing was incomplete. I pulled the change tickets, compared them to deployment logs in Splunk, and confirmed the gap was not isolated. I raised it with the IT change manager first to understand the cause, then documented the finding with examples and a risk rating. I also spoke with the financial auditor because the system affected statutory reporting. Management accepted the finding and introduced a monthly review of emergency changes by the change advisory board, with evidence retained in the ticketing system. I followed up the next quarter and tested a sample to confirm the new control was operating.”

3. You are testing access controls and find a user with excessive privileges in a payroll system. What do you do?

Why they ask
This tests judgement under pressure, confidentiality and how you apply professional scepticism without jumping to conclusions.

How to structure your answer
Use a judgement under pressure structure: confirm the facts, check the criteria, preserve evidence, escalate through the right channel, assess the risk, recommend action and plan a retest.

Example answer

“First I would confirm the facts without making assumptions. I would check the user's role, their approved access request, the role matrix and whether their duties require those privileges. I would preserve the evidence by taking dated screenshots or exporting the access listing. If the access is not approved, I would treat it as a potential exception and raise it with the audit manager before discussing it with the process owner. I would not share the finding widely or name the individual in open forums. I would assess the risk, for example whether the user can alter pay rates or approve their own transactions, and document the impact. Then I would discuss a recommendation with management, such as removing the excess access and reviewing similar accounts. I would follow up to confirm the access was changed and retest.”

4. How would you test the effectiveness of a change management control over a financial system?

Why they ask
This probes your practical testing skills and whether you can move from a control description to a defensible conclusion.

How to structure your answer
Use a testing walk-through structure: control objective, population, sampling or data analytics, evidence inspected, exception handling and conclusion.

Example answer

“I would start with the control objective, which is that changes to the financial system are authorised, tested and approved before deployment, and that emergency changes are reviewed afterwards. I would obtain the population of changes for the period from the ticketing system or deployment logs. If the population is large, I might use ACL to identify high-risk changes, such as those affecting calculation logic or interfaces. I would inspect the change request, approval, test evidence,

deployment record and post-implementation review. For a sample, I would trace each item through the workflow. I would also check segregation of duties between developer and deployer. If I found missing approvals, I would expand testing to determine whether the exception is isolated. I would document the criteria, the evidence and my conclusion for each item, then report any control gaps with a recommendation."

5. Describe your experience assessing compliance with a framework such as ISO/IEC 27001 or APRA CPS 234.

Why they ask

This assesses whether you can work with Australian and international regulatory expectations and map them to real controls.

How to structure your answer

Use a framework mapping structure: state the framework, explain how you mapped controls, describe evidence tested, identify gaps and show how you tracked remediation.

Example answer

"I have assessed controls against ISO/IEC 27001 and used its Annex A controls to structure a gap review. I worked with system owners to map existing policies and procedures to the controls, then tested evidence for areas like access review, incident management and supplier security. For APRA CPS 234, I have reviewed how an organisation maintained an information security capability, classified assets and tested controls, and how it notified material incidents. I focused on whether the evidence supported the control description rather than just whether a policy existed. Where gaps appeared, I worked with the owner to agree a remediation action and a due date. I also tracked findings in a register and reported progress to the audit committee until closure."

6. How do you explain a technical audit finding to a non-technical finance manager or board?

Why they ask

This checks whether you can communicate risk clearly and influence people who do not work in technology.

How to structure your answer

Use an audience-first structure: business impact, plain-language explanation, evidence, recommendation and invitation for questions.

Example answer

"I start with the business impact, not the technical detail. For example, instead of saying a service account had domain admin rights, I would say that a shared account could change financial records without an individual approval trail, which affects the reliability of reporting. I explain how we tested the control, what we found and what could go wrong in plain terms. I use a short example and avoid jargon or acronyms unless the audience uses them. I present the risk rating and the recommendation, and I invite questions so we can agree on a practical response. I also make sure the written report can stand alone, with a clear finding, criteria, cause, effect and recommendation."