CHARTA LEARNING · INTERVIEW PREPARATION

Internal Controls, IT and Fraud

Interview preparation summary · AU track

IN THIS SUMMARY

- Controls
- IT and fraud

INT.UC.1.a · Controls

Name the components of internal control, explain what an auditor does in a walkthrough, and say what a walkthrough does and does not show.

Internal control is the set of processes that management and those charged with governance use to keep reporting reliable, operations effective and laws followed. Auditing frameworks usually describe five components: the control environment (the tone set by management and its attitude to controls), the entity's own risk assessment process, the information system and communication, control activities such as approvals, reconciliations and system checks, and monitoring. The auditor must understand the controls relevant to the audit, which means judging whether each is designed to prevent or detect a material misstatement and whether it has actually been put in place. The usual tool is a walkthrough: follow one transaction from start to finish, asking the people involved, inspecting the documents and observing the step. A walkthrough shows design and implementation for one item. It does not show that the control worked all year; that needs testing. Candidates often list the five components and stop. Say which control matters to which risk.

WORKED EXAMPLE: WALKING ONE PURCHASE THROUGH KESTREL PACKAGING

Kestrel Packaging is an invented manufacturer. Its policy says the system matches each supplier invoice to the purchase order and goods received note, and any invoice more than 2.0% above the order value must be approved by the purchasing manager before payment. You walk through one resin invoice of 18,450 against a purchase order of 18,000. Decide what the walkthrough shows. Convention: variance is measured against the order value.

Answer: The match and tolerance control is well designed, but the walkthrough found one 18,450 invoice, 2.5% above order, paid without the required approval. Design is adequate, implementation is in doubt for this item, and operating effectiveness is untested. Next step: find out how often overrides happen, then test or stop relying.

> **Interview tip:** Say what you did, what you found, and what it does not prove. Finish with the next step: test the control properly or plan to test the balance directly.

INT.UC.1.b · Controls

Distinguish tests of controls from substantive procedures, evaluate a deviation rate against a tolerable rate, and say when an auditor can rely on controls.

Tests of controls ask whether a control operated effectively throughout the period, who performed it and how consistently. Substantive procedures test the balances, transactions and disclosures directly. An auditor tests controls when intending to rely on them to reduce substantive work, or when substantive procedures alone cannot give enough evidence, as with a highly automated sales process leaving little paper trail. Inquiry alone is not enough; it is combined with inspection, observation or reperformance. The sample size is driven by how often the control operates, the tolerable deviation rate, the rate expected and the risk the control addresses. If the sample deviation rate is above the tolerable rate, the auditor cannot rely as planned and must widen substantive testing. A clean result does not remove substantive work on material balances or significant risks. Common mistakes are testing a control and then leaving the substantive plan unchanged, and treating a passed control test as proof the balance is right.

WORKED EXAMPLE: TESTING DISCOUNT APPROVALS AT MARLOW TEXTILES

Marlow Textiles is an invented clothing wholesaler. A control requires the commercial director to approve any customer discount above 5,000. There were 1,200 such discounts in the year. The auditor tests a sample of 25 and finds that 2 have no approval. The tolerable deviation rate is 5.0% and the planned substantive sample for discounts is 30 items if the control is relied on and 50 if it is not (illustrative firm guidance). Decide whether to rely. Convention: non-statistical sample, point estimate only.

Answer: The deviation rate is 8.0% against a tolerable 5.0%, so the control cannot be relied on as planned. The substantive sample goes from 30 to 50 items and the cover gap is reported to management.

> **Interview tip:** State the rate, the threshold and the consequence in that order, then say you asked why the deviations happened. The cause often matters as much as the number.

INT.UC.1.c · Controls

Evaluate a control deficiency by its potential effect, explain how it is communicated, and apply segregation of duties with compensating controls.

A control deficiency exists when a control is missing, badly designed or not operating. The auditor judges how serious it is by the likelihood and the possible size of a misstatement it could allow, not by whether one has actually occurred, and takes account of any compensating control that would catch the problem. A deficiency important enough to deserve the attention of those charged with governance is usually called significant; some regimes use stronger labels for listed companies, and practice varies by jurisdiction. Auditing standards require significant deficiencies to be communicated in writing to those charged with governance on a timely basis, and other deficiencies to management at an appropriate level. Segregation of duties separates authorising, recording, holding assets and reconciling, so no one person can commit and hide an error or fraud. A small team may rely on owner review instead. The mistake is to dismiss a deficiency because it is small against materiality, or because management promises to fix it.

WORKED EXAMPLE: ONE PAYROLL CLERK AT EASTMOOR CARE HOMES

Eastmoor Care Homes is an invented provider. One payroll clerk can add employees, change bank details and run the payment file. In the year there were 62 bank detail changes, and the auditor finds that 9 have no signed form. The average monthly net pay of those 9 employees is 2,150. Overall materiality is 1.5m and performance materiality is 1.125m. The finance director reviews a monthly payroll variance report. Evaluate the deficiency. Convention: exposure is nine employees paid for twelve months.

Answer: Nine of 62 changes, 14.5%, had no form, with a possible exposure of 232,200, about 15% of materiality. Size alone would not make it material, but one person controlling payee creation and payment is a fraud route, so it is reported in writing as significant.

> **Interview tip:** Say that size against materiality is only one test. Add who could exploit it and what compensating control exists, then say it is reported in writing.

INT.UC.2.a · IT and fraud

Distinguish IT general controls from application controls and explain why weak general controls limit reliance on automated controls and system reports.

Most clients run their accounting on IT systems, so an auditor looks at two layers of control. IT general controls cover the environment: access management (who can log in and what they can do, including joiners, movers, leavers and privileged accounts), change management (whether program changes are authorised, tested and approved before going live) and IT operations (backups, job scheduling and incident handling). Application controls sit inside a process: input validation, an automated three-way match, calculations, interface checks and exception reports. An automated control that works once usually works the same way every time, so the auditor can test it once and rely on it, but only if the general controls show it has not been altered or bypassed. The same applies to reports the client produces and a manager then reviews. Weak general controls mean the auditor cannot assume this and must test more directly. The common mistake is testing the application control without looking at the controls around it.

WORKED EXAMPLE: ACCESS AND CHANGE CONTROLS AT HARBOUR FOODS

Harbour Foods is an invented distributor. Its ERP has 52 users, 6 with privileged access. 31 staff left in the year and 4 of their accounts were still active at year-end. There were 18 changes to the invoice matching module and 3 had no approval evidence. The auditor wants to rely on the automated three-way match. Decide what the numbers mean. Convention: percentages to one decimal place.

Answer: Four of 31 leavers still had access (12.9%) and 3 of 18 changes to the matching module had no approval (16.7%). The general controls are weak, so the three-way match cannot be relied on without more work.

> **Interview tip:** Explain the dependency in one sentence: an automated control is only as reliable as the access and change controls around it. Then give the numbers.

INT.UC.2.b · IT and fraud

Apply the fraud triangle to a client, separate fraud risk factors from evidence of fraud, and explain why revenue is presumed to be a fraud risk.

The fraud triangle says fraud usually needs three things: an incentive or pressure, such as a bonus target or loan covenant; an opportunity, such as weak controls or the power to override them; and a way to rationalise it, such as believing a sale is only early, not false. Risk factors differ for fraudulent financial reporting, where the aim is to mislead users of the statements, and misappropriation of assets, where the aim is to steal. Management and those charged with governance are responsible for preventing and detecting fraud. The auditor obtains reasonable assurance that the statements are free of material misstatement, whether from fraud or error, but fraud is harder to find because it involves concealment, forged documents and collusion. Auditing standards presume a fraud risk in revenue recognition, which the auditor may rebut only with reasons. A risk factor is not proof of fraud. The common mistake is to treat the triangle as a checklist and not use it to choose procedures.

WORKED EXAMPLE: BONUS PRESSURE AT LORNE INSTRUMENTS

Lorne Instruments is an invented maker of lab equipment. Last year revenue was 111.0m. The executive bonus pays only if revenue grows by at least 8.0%. Draft revenue is 119.95m. Sales booked in the last five working days total 3.6m (1.1m in the same days last year), mostly invoiced manually and approved by the sales director. Identify the risk and measure the margin of safety.

Answer: The bonus needs revenue of 119.88m and draft revenue is 119.95m, leaving 70k, only 1.9% of the 3.6m booked in the last five days. That is pressure and opportunity together, so I would test cut-off hard.

> **Interview tip:** Name all three sides of the triangle with evidence from the case, then say the procedure you would choose. Do not say the client is committing fraud.

INT.UC.2.c · IT and fraud

Explain why management override is always a risk, describe how journals are selected for testing, and set out what an auditor does and does not do when fraud is suspected.

Management can override controls that look effective, so auditing standards treat the risk of management override as present in every audit. Whatever else the risk assessment says, the auditor tests the appropriateness of journal entries and other adjustments, reviews accounting estimates for bias and evaluates the business reason for significant unusual transactions. Journals are selected by risk characteristics: manual entries, posting at or after period end, round amounts, unusual account pairings, entries by senior users or with no description. Software lets the auditor test the whole population and narrow it. If fraud is suspected, the auditor discusses it with the manager and partner, raises it at an appropriate level of management (above any person implicated), tells those charged with governance, reassesses the risks and the reliability of representations, and takes advice on any duty to report, avoiding tipping off. The auditor does not make legal findings of fraud. Many candidates forget that confidentiality is limited by law.

WORKED EXAMPLE: JOURNAL TESTING AT PENHALLOW RETAIL GROUP

Penhallow Retail Group is an invented retailer. There are 14,200 journals in the year, 3,850 of them manual. Of the manual ones, 612 were posted in the last three days of the year or the ten days after. Of those, 148 were round thousands, 41 of those credited revenue or released provisions, and 9 of those were posted under the finance director's user ID with amounts (thousands) of 600, 450, 380, 250, 500, 300, 280, 220 and 280. Overall materiality is 2.4m. Narrow the population and decide the next step.

Answer: Starting with 14,200 journals, the risk criteria leave 9, posted under the finance director's ID, worth 3.26m, which is 1.36 times materiality. I would test all nine, and escalate to the manager and partner if the reasons are not credible.

> **Interview tip:** Describe the funnel as criteria, not as proof. Say you would test every remaining journal, and name who you would tell if the explanation does not hold.

Summary of the Charta interview-preparation topic. Companies and figures in the examples are invented. Draft content, not yet expert reviewed.