

The Interview Case Workbook

Read the record. Explain the decision. Revise when the facts change.

02

ORIGINAL CASES AND WORKED REASONING

Editable practice companions included

Expanded cases and browser-editable working pack

CONTENTS

Your route through the work

Explain a decision someone else can examine	3
The access review that leaves two questions open	7
Joiners, movers and disputed approval	10
The emergency change approved the next morning	15
Two services, different consequences	18
The vendor report that does not cover the proposed service	21
Write the finding the records support	24
A deadline, a disagreement and a decision owner	27
Present an educational project honestly	30
Two timed mock interviews	32
Build your story bank and next practice session	36
The restore finished but the service did not return	39
Prioritize vulnerabilities without outsourcing judgment to a score	42
The dashboard improved because the denominator changed	45
A clean sample from an unclear population	47
The exception expires before the replacement is ready	49
Keep the incident record useful while facts change	51
Three answer clinics for the same facts	54
A third mock: explain the operating picture	56

CASE WORKBOOK / 01

Explain a decision someone else can examine

Using this expanded edition

Chapters 1-11 establish the response method and initial cases. Chapters 12-19 broaden practice to recovery, prioritization, metrics, sampling, exceptions and incident coordination, with a third timed mock. The companion archive includes [START-HERE-working-pack.html](#): open it in a browser to edit the supplied tools, save a local working copy or print. Changes are not saved until you use the save control. Markdown and CSV originals remain available for text editors and spreadsheet software. Keep your own attempt separate from completed references.

This workbook is for candidates who can recognize basic security terms but want more practice explaining a decision. The work is deliberately ordinary: an incomplete access review, a joiner account with unclear approval, an emergency change and a supplier whose evidence does not answer the question being asked. These situations let you practice scope, evidence and communication without pretending to have performed a real assessment.

Every organization, record, conversation and candidate response in the cases is fictional. The questions were written for this publication. They are not leaked questions, accounts of a named employer's interviews or a certification examination bank. A real employer may assess different knowledge and use different terminology. Use the cases to improve your reasoning, then prepare for the responsibilities in the actual posting.

What you should bring

You should be comfortable with the idea that a system has users, permissions and administrators; that a change can alter how it works; and that a business depends on the availability and appropriate use of its information. You do not need to recite a catalog of control identifiers. When a term in a case is unfamiliar, pause and define it before trying to answer quickly.

Keep a notebook or use the response companion. For each attempt, record your initial answer before opening the worked reasoning. The first version is useful evidence of your preparation. If you replace it immediately with a polished answer, you lose the opportunity to see which assumption caused the difficulty.

The workbook's response structure is an editorial aid, not an official standard: identify the decision, establish the facts, state the limitation, recommend the next action and explain who owns it. You can change the order to suit the question. A short factual answer can be stronger than a speech that mechanically visits every heading.

Start by identifying the decision

“Is the supplier safe?” sounds like one question, but it can conceal several decisions. May a team experiment with a tool using synthetic data? May the supplier process customer information? May it connect to production systems? Who can authorize each step, and what evidence is needed? An answer that assumes the broadest or narrowest interpretation without saying so may solve the wrong problem.

In a practice interview, ask one or two questions that would materially affect the recommendation. Do not use clarification as a way to postpone all judgment. If the interviewer cannot provide more detail, state a reasonable assumption and show how the answer would change if the assumption were wrong.

For example: “I will assume the proposed integration has read access only to the pilot workspace, not the production document store. If it also has production access, I would expand the scope before supporting the pilot decision.” The assumption is now visible. Another person can challenge it rather than unknowingly relying on it.

Separate observation from interpretation

A worksheet containing a reviewer’s name is an observation. “The reviewer considered every privileged account” is an interpretation that needs more support. A ticket closed on Friday is an observation. “Access was removed on Friday” may require a source record showing that the ticket corresponds to the implemented action.

Use careful language when you cross that boundary. “The package records” is different from “I independently confirmed.” “This suggests” is different from “This establishes.” These phrases should reflect genuine differences in your evidence, not make every sentence evasive.

Consider a candidate who says, “The vendor passed the access control because the worksheet is signed.” A stronger explanation would identify what the signature supports and what remains to examine: the covered service, account population, review period, criteria and open exceptions. The signature is useful; it simply does not answer every question.

Use a criterion before declaring a deviation

The cases provide fictional policies where a timing or approval criterion matters. Read them. Do not replace a stated two-business-day requirement with a personal belief that everything must happen immediately. Equally, do not assume that an activity satisfies a requirement merely because it eventually happened.

Suppose a fictional procedure requires an independent approver before a normal production change. A ticket approved after the change raises a different issue from a procedure that explicitly permits retrospective approval for an emergency. You need the applicable path, the actual dates and the evidence connecting them.

NIST SP 800-53A distinguishes assessment methods including examining material, interviewing people and testing mechanisms. Its procedures are selected and tailored for the assessment’s purpose and assurance needs. The workbook does not reproduce that methodology or turn its fictional exercises into formal

assessments. The practical lesson here is narrower: explain what action would produce the evidence your question requires, rather than listing every possible document and interview.

Recommend a next action with an owner

“Investigate further” is rarely a complete recommendation. Specify what you need, why it matters, who can supply it and what decision is waiting. A useful request might ask the identity-system owner to explain how a population was generated and reconcile it with the service's administrator list. That is more focused than asking for “all access documentation.”

The person evaluating evidence may not be the person authorized to accept a risk, approve a supplier or change production access. Make that boundary clear. You can recommend a restriction or escalation without pretending that you own the final decision. If the scenario does give you authority, explain the basis and conditions of the decision you would make.

Time matters as well. A request with no deadline can remain unresolved indefinitely. State the business decision date and a reasonable review point. In a real role, agree timing with the responsible team and follow the organization's process; do not invent a mandatory deadline from this exercise.

Practice: revise a weak answer

Prompt: “A quarterly access review has two unresolved accounts. Can the team proceed with a pilot?”

Weak answer: “I would mark it high risk, reject the vendor and tell them to fix the control.”

Before reading further, identify three missing pieces. A strong diagnosis notices that the answer does not define the pilot, does not explain the account questions and does not identify the decision owner. It also assigns a risk rating without criteria and treats incomplete evidence as a confirmed failure.

A possible revision: “I would first confirm the pilot’s data and access scope. The review leaves two account decisions unresolved, so I would request the supporting disposition and check the population covered. I would give the decision owner a scoped recommendation with any unresolved conditions, rather than treating that one record as approval or rejection of the entire supplier.”

This is not the only valid answer. A different fact could make immediate escalation appropriate: an account known to belong to a departed administrator, for example, would change the concern. Your task is to explain which fact drives which action.

Record the change in your reasoning

After each case, finish these three sentences in your own words:

- My first answer assumed that...
- The evidence actually supported...
- Next time, I will clarify or request...

Keep the response specific. “I need to be more confident” is less useful than “I treated the export as complete without asking how it was generated.” The second observation gives you something concrete to change in the next attempt.

Source note: NIST SP 800-53A revision 5, sections 2.4 and 3.2, provides formal assessment background. The structures, prompts and answers in this chapter are original teaching material. [Read the publication.](#)

CASE WORKBOOK / 02

The access review that leaves two questions open

Morrow Services is evaluating Finch Documents, a fictional document-processing supplier. Sixty employees want to try a pilot using synthetic documents. A separate proposal would allow customer documents later. The business owner asks you to review the supplied access evidence before the team discusses those decisions.

You are a candidate practicing an analyst's explanation. You are not the authorized approver, and this packet is not a complete supplier assessment. Focus on what the access records support, what they leave unresolved and how you would communicate the result.

The supplied records

EV-01 is a policy dated 12 January. It says the security lead reviews privileged access quarterly and that exceptions should have a named owner and due date. It does not specify in this extract how the account population is generated or when the review must finish after quarter-end.

EV-02 is a spreadsheet dated 30 June. It lists eighteen privileged account IDs and their roles for the document service. It does not include source-query parameters, an extraction log or a reconciliation to another inventory. The sender has not explained whether service accounts are included.

EV-03 is a review worksheet dated 2 July. A named reviewer accepted sixteen accounts and marked two for owner confirmation. It contains no links to the follow-up tickets and no later evidence of closure. The package does not include the criteria the reviewer used to judge appropriateness.

Keep the arithmetic simple: sixteen accepted and two unresolved accounts total eighteen listed accounts. This reconciles the worksheet to the supplied list; it does not establish that the list represents every account in scope.

Your first attempt

Take five minutes to produce four short items:

1. The decision you believe is being requested, including any ambiguity.
2. One statement that the supplied packet supports.
3. Three targeted questions that would change your assessment.
4. A provisional next step with a responsible owner.

Do not assign a numerical score. You do not have a defined rating method, information about all service risks or authority to make the final supplier decision. Practice describing the uncertainty accurately before compressing it into a label.

Worked analysis

The packet supports a narrow statement: it records review activity for eighteen listed accounts, with two decisions unresolved in the supplied worksheet. It also documents an expectation for quarterly review. It does not yet establish complete coverage, appropriateness of every account or resolution of the two questions.

The first targeted question concerns scope: which service components and account types were included, and how was the population produced? Ask the supplier to provide an explanation or suitably redacted supporting record. An entire user database is not automatically necessary. The evidence request should seek enough information to understand completeness without collecting unrelated personal data.

The second concerns criteria: how did the reviewer determine whether access was appropriate? A role name alone may not show business need or the scope of privileges. The third concerns follow-up: what happened to the two accounts, who owns each decision and when was it resolved or escalated?

You should also clarify the pilot separately from the customer-data proposal. A synthetic-data pilot may have a different exposure, but it is not automatically harmless. It might introduce an integration, credentials or access paths that matter even without customer documents. Ask what will actually be connected and what restrictions can be enforced.

A decision note you could explain

“The packet documents an access review of eighteen listed accounts and identifies two unresolved account decisions. I have not established the completeness of that population or obtained the subsequent disposition of the two items. I recommend asking the supplier's security contact for the population scope, review criteria and closure records. The business owner should distinguish the proposed synthetic-data pilot from later customer-data use and consider these limitations alongside the other supplier-review work before authorizing either scope.”

Notice the note's boundaries. It does not say the supplier is compliant, that two unauthorized accounts exist or that the analyst has approved the pilot. It identifies the evidence gap and the decision that must take it into account.

Why the tempting alternatives fail

“Approve because most accounts were accepted” treats a count as a risk measure. The two unresolved accounts might be harmless duplicate records, or they might carry significant privileges. The supplied information does not tell you which. A percentage such as sixteen out of eighteen can describe the worksheet, but it cannot settle appropriateness or risk.

“Reject because two accounts failed” changes the worksheet's wording. The record says owner confirmation is needed. That is not equivalent to a documented inappropriate-access finding. Escalation may still be necessary if the decision deadline arrives before the evidence does, but the reason should remain accurate.

“Ask for everything” avoids choosing the evidence that matters. It can delay the review and expose unnecessary information. A targeted request makes it easier for the supplier to respond and for another analyst to understand why the material is relevant.

Follow-up one: the supplier supplies more records

The supplier explains that the export includes named human administrators but excludes service accounts. It provides closure tickets for the two human accounts: one duplicate record was removed from the worksheet, and one temporary access grant was ended on 5 July. A separate register lists four service accounts, but no service-account review is included.

Revise your analysis. The two human-account questions now have supporting follow-up, subject to checking that the tickets correspond to the supplied records. The original population was narrower than you might have assumed. Ask whether the review requirement covers the service accounts, who owns them and what process evaluates their privileges. Do not silently expand the eighteen-account result to cover the additional four.

The duplicate record also means you should be careful about counting unique accounts. Eighteen rows may not mean eighteen distinct active identities. Record the explanation rather than retroactively pretending that the first packet was unambiguous.

Follow-up two: the deadline arrives

The business owner says the pilot must begin tomorrow, but the service-account evidence will take a week. Prepare options rather than a false binary. One option may be to defer the decision. Another may be to narrow the pilot, if the proposed restrictions actually avoid the unresolved exposure and can be implemented. A third may be a documented exception through the organization's authorized process.

For each option, state what remains uncertain and who can decide. Do not recommend a technical restriction without asking someone responsible for the implementation to confirm it. “No customer data” is a policy statement unless the workflow actually supports that boundary and people understand it.

Self-review and companion work

The evidence-register companion contains a completed reference for EV-01 through EV-03. Make a working copy, compare each row with the original packet, then add the follow-up items with new IDs. Preserve the original limitations and show which ones the later records address. Write a revised note of no more than 180 words.

Your work is ready to discuss when another reader can trace each conclusion to a record or an explicitly labeled assumption. If the reader cannot tell which evidence changed your mind, revise the note before making it more polished.