

Your first IAM business case

15 scenario questions + an Acme Corp exercise + safe AI review

By Manmeet Dhanesar

For IT professionals exploring identity and access management. No software installation is required. All identities and business scenarios are fictional. Allow 25-35 minutes for the starter exercise.

Five ideas to understand

Authentication

Establish who is signing in. Bob completes sign-in and MFA.

Authorization

Decide what an identity may do. Bob can view reports but cannot approve payments.

Provisioning

Create and update accounts and access. Alice receives an approved directory account.

Governance

Review and justify access. A manager removes stale entitlements.

Privileged access

Control powerful administration. A separate admin identity manages a scoped lab OU.

SSO reduces repeated authentication across configured applications. It does not automatically grant every application permission.

Practise the lifecycle

Alice joins Marketing tomorrow. Bob moves from Marketing to Finance today. Casey's contractor engagement ends today. Acme's approved HR record is the source for these changes.

- Write the appropriate access change for each person.
- Identify one failure for each change.
- Describe the evidence needed from the target system.
- Explain why a successful HR update alone does not close the request.

Person	Expected change	Possible failure	Target evidence
Alice			
Bob			
Casey			

Self-check

Alice receives approved access at the effective start time. Bob gains approved Finance access and loses obsolete Marketing access. Casey follows the termination procedure, with downstream verification.

Check active cloud/application sessions separately: disabling a directory account does not prove every session has ended. Evidence should identify the person, target, action, time and observed result.

Check your reasoning

Mini lifecycle checklist

- Is the request approved and the effective time clear?
- Is the identity correlated using a stable identifier?
- Is each access grant justified by a role or an approved request?
- Did the change reach every relevant target?
- Did the allowed and denied test cases behave correctly?
- Were failures resolved and the final state documented?

AI review exercise - optional

Use only fictional information. Ask an AI assistant:

"Suggest a test checklist for Bob moving from Marketing to Finance. Identify assumptions and include a test for obsolete access. Do not invent vendor commands."

Inspect its response. Did it forget removing old access? Assume immediate synchronization? Treat authentication as authorization? Correct at least one weakness and explain why.

Without AI, critique your own checklist using the same questions. A paid AI account is not required.

Do not submit real employee data, credentials or complete tokens to public AI tools.

Explain the business outcome

Threat → Risk → Identity → Control → Outcome

Example: a departed contractor retains access → information may be exposed → Casey's target account remains active → remediate deprovisioning and supported sessions → show rejected access and target-side evidence.

15 IAM scenario questions

1. Alice starts tomorrow. Should her account work today, and what controls the effective time?
2. Two HR records share an employeeid. What should happen before provisioning?
3. Bob moves departments. Which access should be added and which should be removed?
4. HR shows Casey as terminated, but the target account is active. What evidence is needed?
5. Casey's account is disabled, but an existing app session works. What do you check next?
6. A user authenticates successfully but cannot view a report. Is this necessarily an authentication failure?
7. A user is assigned to an SSO app but the SAML audience is wrong. What would you investigate?
8. A token is readable but expired. Does decoding it establish that it should be trusted?
9. An access request has no business justification. What should the reviewer do?
10. One person can create vendors and approve payments. What risk does that create?
11. A registered device is not compliant. Should you treat the two states as equivalent?
12. A policy is in report-only mode. Does its predicted block prove actual access was blocked?
13. A manager approves keeping stale access without reviewing it. Is the review complete?
14. A caller sounds like an executive and requests an urgent MFA reset. What independent verification is needed?
15. AI suggests granting a broad administrator role to solve a small issue. How would you verify and improve the recommendation?

For each question, explain the business risk, proposed control and evidence needed. These are learner prompts, not a certification assessment.

Continue learning with Manmeet Dhanesar: cyberiamacademy.com

Educational material; no employment or certification guarantee. Personal learning and sharing this unchanged guide with attribution are permitted; resale is not. Version 1.0 - October 2026.