# Questions to Ask

A takeaway from the masterclass with **Espen Bago** & **Lance Peterman**.
Two questions per topic: one to **deepen your understanding**, one to **challenge your assumptions**. Take them back to your team. · **identi.beer/intro**

## 01 Foundations

**DEEPEN YOUR UNDERSTANDING**
What does your organization consider the core identity relationships it needs to represent? Who is accountable for keeping that current?

**CHALLENGE ASSUMPTIONS**
If you automated every access decision tomorrow, what data would you not have to do it well?

## 02 Objects & Contexts

**DEEPEN YOUR UNDERSTANDING**
In your organization, which identity contexts — workforce, customer, citizen, partner, machines — are managed by the same team, and which are siloed?

**CHALLENGE ASSUMPTIONS**
Are you treating the same person differently across contexts because it serves the business — or because your data is siloed and nobody noticed?

## 03 Perspectives

**DEEPEN YOUR UNDERSTANDING**
Which perspective dominates your IAM conversations — security, privacy, business enablement, or architecture? Which one is missing from the table?

**CHALLENGE ASSUMPTIONS**
When your IAM team talks to the business, do they speak the business's language — or do they expect the business to learn IAM's?

## 04 Governance

**DEEPEN YOUR UNDERSTANDING**
How much of your entitlement catalog has meaningful descriptions and named owners — not GRP_FIN_LEGACY_03 with nobody attached to it?

**CHALLENGE ASSUMPTIONS**
When a manager certifies someone's access, do they have the information to make a real decision — or are they rubber-stamping because that's the only option you've given them?

## 05 Privileged Access

**DEEPEN YOUR UNDERSTANDING**
How does your organization define what's "privileged" — is it formally documented, or is it whatever your security team decided last quarter?

**CHALLENGE ASSUMPTIONS**
Does "privileged" include the application owner who can change access rules in their own app — or just the sysadmin who runs the OS underneath it?

## 06 Admin-time vs Run-time

**DEEPEN YOUR UNDERSTANDING**
Look at your IAM decisions: which happen admin-time, which happen run-time? Is the balance deliberate or accidental?

**CHALLENGE ASSUMPTIONS**
When a policy changes, how long before every enforcement point is using the new version? Do you actually know — or are you assuming?

## 07 Authentication

**DEEPEN YOUR UNDERSTANDING**
Look at your MFA setup: are the factors actually independent — or are "something you have" and "something you are" both stored on the same phone?

**CHALLENGE ASSUMPTIONS**
If an attacker had a convincing deepfake of your CEO's voice and called your helpdesk, which of your authentication or recovery processes would still hold up?

## 08 Authorization

**DEEPEN YOUR UNDERSTANDING**
Where are your authorization decisions made — inline in each application, or through an externalized decision service? How do you keep policies consistent across them?

**CHALLENGE ASSUMPTIONS**
When a vendor says their product "does RBAC" or "does ABAC" — do you know whether they built externalized authorization, or just hardcoded some role checks?

## 09 AI & Identity

**DEEPEN YOUR UNDERSTANDING**
When an AI agent takes action on behalf of a user, what's recorded in the audit log — the agent, the user, both, or just "system"?

**CHALLENGE ASSUMPTIONS**
How many AI agents are running in your organization right now? Who owns each one, and what happens when those owners leave?