

ACCESS AUTHORIZATION GAP

ARCHITECT'S REVIEW QUESTIONS

Run these against any control in your environment that gates access to a sensitive resource by asking the requester to confirm their own authorization.

1

Does this control verify access, purpose, or both?

2

Who or what supplies the evidence of purpose — the requester, the system, or an independent party?

3

Can the requester control or influence that evidence?

4

What happens if the self-attestation is false? Is anything stopped, or only logged?

5

Is the control preventive, or merely auditable after the fact?

6

Where is purpose authorization independently established — engagement, ticket, case, or business context the requester didn't produce?



RACK2CLOUD
Think Like An Architect.
Build Like An Engineer.

Think Like An Architect. Build Like An Engineer.