AGENTIC AI · BEFORE YOU SIGN

Your AI contract says no. *Can the agent still do it?*

A contractual restriction and a technical control are not the same thing.

1 What is the agent allowed to do?

Read → **Draft** → **Send** → **Accept** Four levels of authority

Define the approved actions, data access, transaction limits and points where a person must decide.

2 What actually enforces those limits?

Don't just ask whether the control exists. **In a test environment, give the agent a task outside its authority** and ask to see what happens.

- ☐ Does the system reject the action before it reaches the supplier or finance platform?
- ☐ What gets logged?
- ☐ Who is alerted?

3 Who owns that control after signature?

LAYER 1	LAYER 2	LAYER 3
What the contract says the agent can do	What the technology can actually block	What controls we configure and turn on

The contract needs to be clear about who sets the limits, who tests them when things change, what evidence we receive, and who acts if something goes wrong.

ASK BEFORE SIGNATURE

Which boundaries exist only in the contract, and which ones will the technology actually enforce?

Not every contractual obligation can be turned into a technical control. Incident notification, cooperation and remedies still matter.

Zina Amir Moafi
Procurement at AI Speed · Episode 3 · **kaizina.com.au**

KaiZina