
Agents need boundaries

When does an assistant become a system that can act?

Use authorised information. Keep personal records in your own controlled workspace.

Tool and permitted action

Identity and data scope

Recipient, amount or destination limits

Pre-execution checks

Approval evidence

Retry and budget caps

Audit trail and recovery owner

Use the example. Then test your own.

INVENTED TEACHING EXAMPLE

A proposal stops at the gate

Synthetic ticket EXAMPLE-004 produces a proposal for £20 store credit. Before the action, a person sees the ticket, amount, policy and reason. Without approval the action remains blocked. After approval the teaching example records a simulated action. No payment, refund or message takes place.

Before treating this as evidence

Record the real inputs, source version and acceptance rules. Compare observed outcomes with the requirement. Keep unknowns and failure consequences visible.

What did you observe?

What remains unknown?

What will you do next—and who owns it?

Method and references: [the web edition's sources and scope](#). This is a practical editorial worksheet, not a certification or validated assessment instrument.