

FRAMEWORK ON ONE PAGE · VERSION 1.0

Chain Authorization Gap

Chain accountability test · August 2026

TIME TO USE 30 min review / 90 min workshop	AUDIENCE Architecture, risk, security, and compliance leaders	OUTPUT A chain-level authorization record
--	--	--

?

The orchestrator may delegate the task. The enterprise cannot delegate the burden of proof. When the examiner asks for the authorization record covering this chain's actions, the Entra Agent ID record is not that document.

What it is

The Chain Authorization Gap is the absence of any authorization record for the outcome of a multi-agent chain, where no single agent in the chain was individually authorized for what the chain collectively did.

A chain-level authorization record is not a policy document. It is not a platform configuration. It is a governance artifact that answers four specific questions, produced before the chain goes live, and maintained for the life of the chain.

The four questions

The Chain Root	Every multi-agent chain originates with a human or system trigger.
The Authorization Root	Authorization for the chain must be documented before the chain executes.
Each Delegation Hop	Every point in the chain where one agent delegates a subtask to another agent is a delegation hop.
The Permitted External Effect Boundary	Before the chain goes live, the authorization record must define the boundary of permitted external effects. Which tools the chain may call.

A worked example

Situation	A generic enterprise uses three agents to classify invoices, request clarification, and recommend payment disposition.
Where it lands	Chain-level approval is missing
Evidence	Each agent has an individual owner, but no record authorizes the combined chain or names who owns the payment consequence.
Gap found	The delegation boundary between the clarification and payment recommendation steps is undocumented.
Next action	Create one chain record, name the consequence owner, and define the approval boundary for each handoff.
Output	A chain-level authorization record.

The one action it produces

A chain-level authorization record

What good looks like

A governed multi-agent orchestration has a chain authorization record produced before the chain executes in production. That record names who approved the chain, defines the aggregate scope of permitted actions across all agents, identifies the human accountable for the chain's output, and documents the re-authorization triggers and review cadence.

What it cannot establish

This object can expose missing chain-level authorization and ownership. It cannot prove that every downstream action was technically prevented or that the aggregate outcome is safe.

CITE AS

Sougata Roy, "Chain Authorization Gap," Version 1.0, August 2026, <https://sougataroy.com/frameworks/multi-agent-accountability>

Sougata Roy · Enterprise AI Governance Research

<https://sougataroy.com/frameworks/multi-agent-accountability>