MCP Dev Summit Nairobi

MCP Meets Enterprise Integration

Where Should the Agent Boundary Live?

Rhoda Mumo

Enterprise Integration & API Engineer

20 November 2026

How far would you let an agent go?

MCP Dev Summit Nairobi

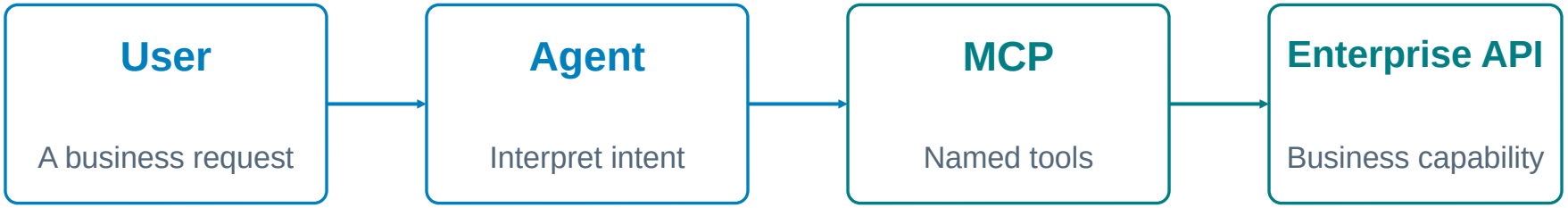
1 Check a supplier’s status

2 Create a supplier

3 Change the supplier’s bank details

Where would you pause for a human decision?

MCP adds a new enterprise consumer



A familiar integration question now applies to an agent:

Which capabilities may this consumer use?

What is a business capability?

MCP Dev Summit Nairobi

A useful task a business system can perform

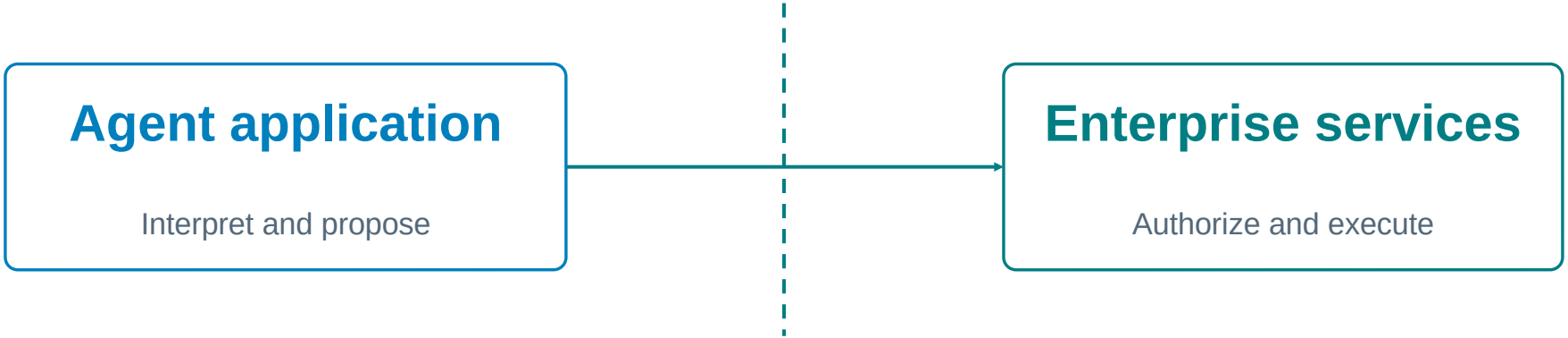
Business task	MCP tool	Implementation
Check supplier status	**get_supplier_status**	**API + database**

The task stays familiar while the systems behind it can change

Where is the agent boundary?

MCP Dev Summit Nairobi

The point where a proposed action meets trusted rules for enterprise execution



Capability contract + authority + an accountable owner

Why identifying the boundary helps

MCP Dev Summit Nairobi

Controlled authority

Limit which data and actions the agent can reach

Reuse of integration work

Keep existing mappings, recovery and API policies

Independent change

Replace models or backends behind a stable capability

Operational ownership

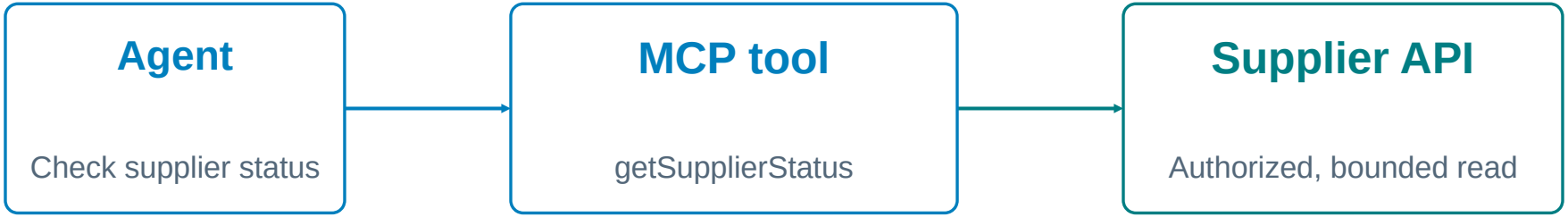
Know who can trace, explain and recover a request

Risks when the boundary is unclear

MCP Dev Summit Nairobi

Design gap	Possible consequence
Broad backend access	The agent reaches unrelated data or actions
System logic in the agent	Mappings and recovery become tightly coupled
Unclear retry semantics	A timeout can lead to a repeated business action
Approval only in the client	Another caller can bypass the approval path

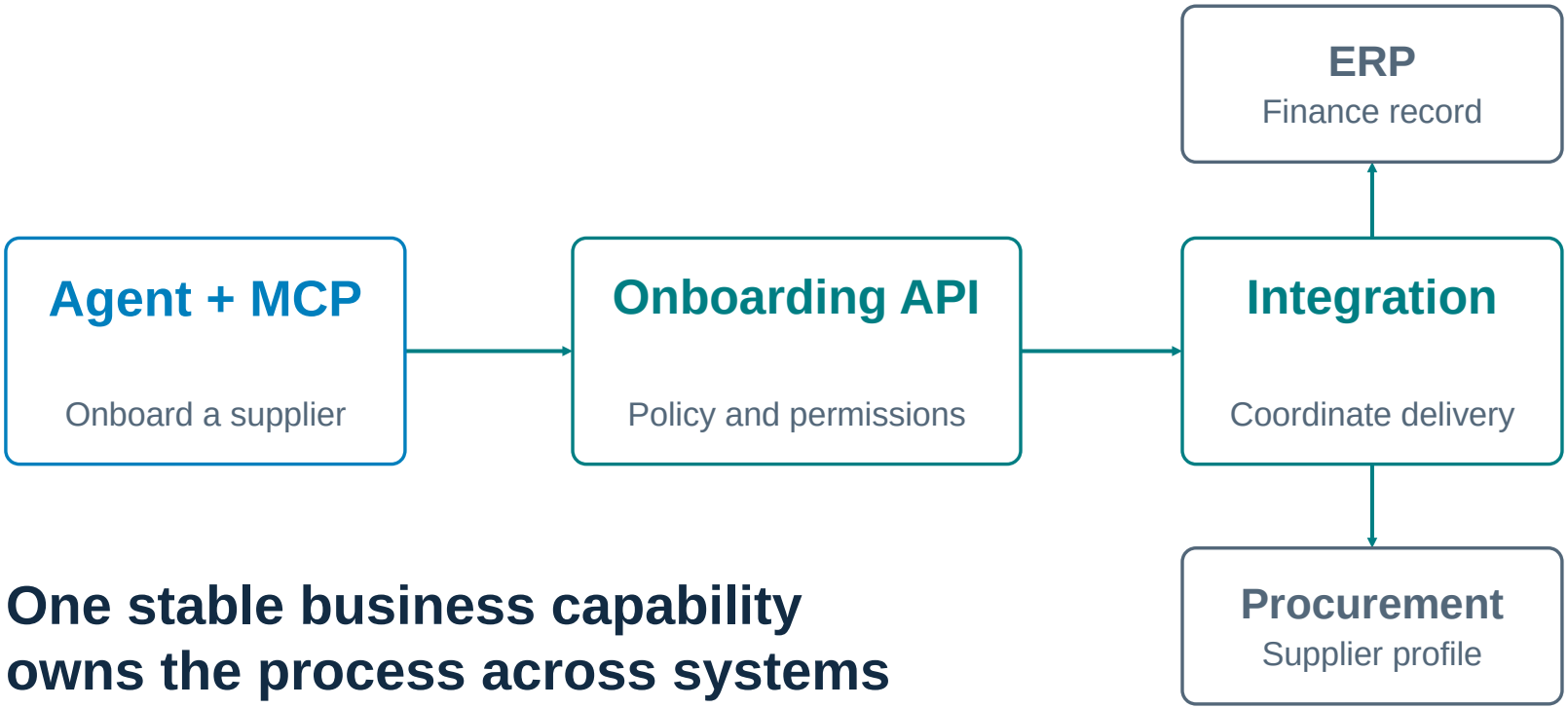
Scenario: direct API access



A clear capability with one owner and predictable behavior

The API still enforces caller and resource permissions

Scenario: enterprise integration



One stable business capability owns the process across systems

Which route would you choose?

MCP Dev Summit Nairobi

A Check the health of one internal API

B Onboard a supplier across finance and procurement

C Change a supplier’s bank details

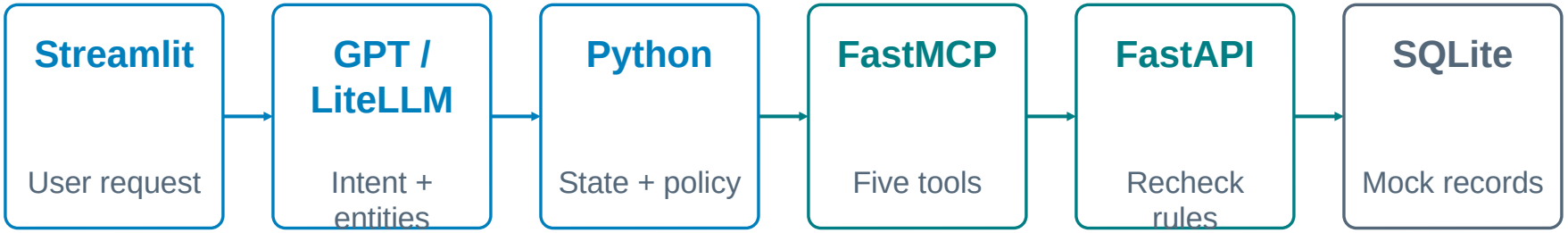
Think about integration complexity and business risk separately

Who owns each part of the request?

MCP Dev Summit Nairobi

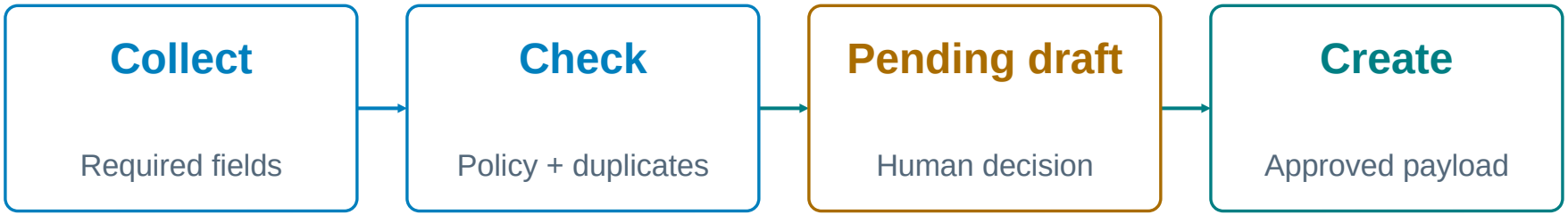
Layer	What it owns
Agent application	Intent and workflow decisions
MCP server	A bounded tool contract and access checks
Capability API	Business authorization and validation
Integration services	Mappings, retries, rate limits and monitoring
System of record	Authoritative transaction and record state

Supplier demo



GPT understands the request.
Python decides the transition and tool call.

Approval is tied to one supplier draft



Questions keep it pending

Corrections trigger fresh checks before approval

Supplier demo: request decisions

MCP Dev Summit Nairobi

User request	Application decision
Show active suppliers in Uganda	Filtered read through list_suppliers
Onboard Techbord in Germany	Refusal before an MCP call
Onboard Acme Technology in Kenya, tax ID ACME123	Duplicate checks, then pending approval
A question about approval	Keep the supplier draft pending

Explicit approval is required before the create tool runs

Boundaries appear in refusals too

MCP Dev Summit Nairobi

Germany onboarding

Unsupported market

→ **Python refuses**

No MCP call

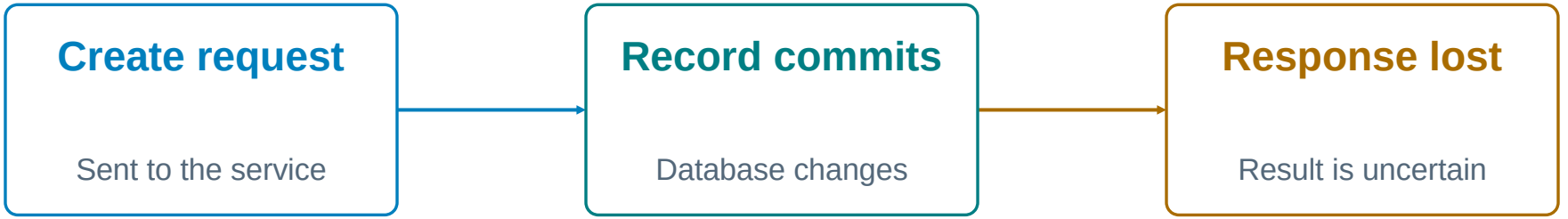
Delete supplier

Unsupported action

→ **Python refuses**

No substitute tool

Failures need a known recovery path



Retries need idempotency or reconciliation

An uncertain outcome needs a truthful user response

Production controls

MCP Dev Summit Nairobi

Identity and permissions

Which caller may perform which action on which record?

Verifiable approval

Did a human approve this exact action and payload?

Durable operation state

What happened, and can a retry safely reconcile it?

Audit and ownership

Who can explain and recover the business outcome?

A framework for your first tool

MCP Dev Summit Nairobi

Capability	What business outcome are we exposing?
Authority	Who may invoke it, and when is approval required?
Execution	Which service owns policy and system complexity?
Evidence	How do we trace, recover and audit the result?

Key takeaways

MCP Dev Summit Nairobi

Business capabilities

Expose clear tasks with limited inputs and results.

Trusted execution

Services enforce permissions, approval and recovery.

Integration ownership

Keep system details behind stable business APIs.

Where would you start?

MCP Dev Summit Nairobi

Business intent for the agent

Controlled execution for the enterprise

Questions



github.com/mumo-rhoda/mcp_supplier_demo

Additional slides: supplier tools

MCP Dev Summit Nairobi

list_suppliers(country?, status?)

search_supplier(name)

get_supplier_status(id)

validate_supplier(name, country, tax_id)

create_supplier(name, country, tax_id)

Additional slides: references

MCP Dev Summit Nairobi

Supplier demo

github.com/mumo-rhoda/mcp_supplier_demo

MCP tools, authorization and security guidance

modelcontextprotocol.io

The demo uses SQLite as a mock enterprise system.
Architecture scenarios do not claim live ERP connections.