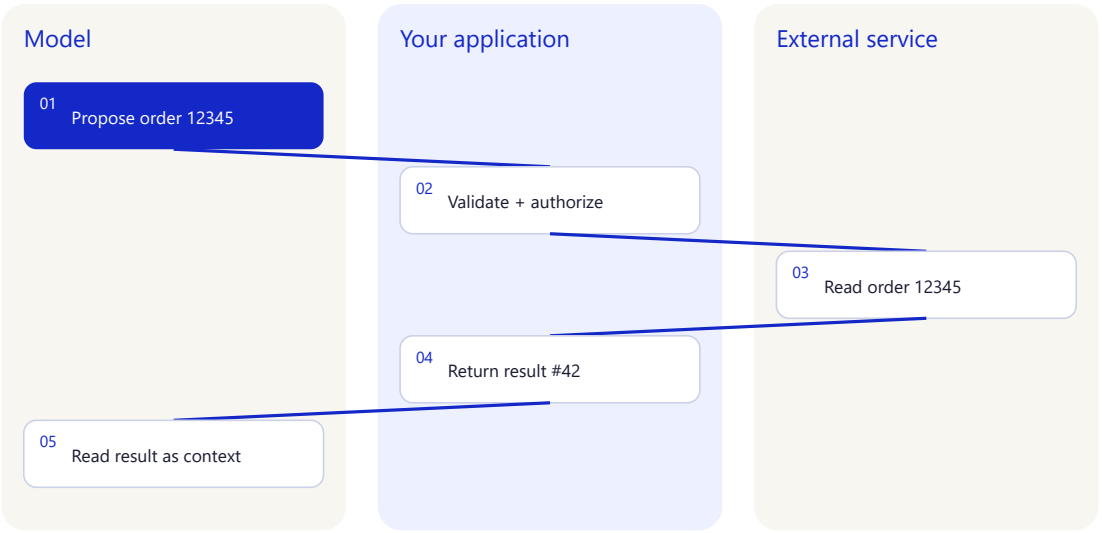
CHAPTER 14 / TOOLS

The model requests. Code decides.

A valid tool call can still be forbidden.

A valid tool call can still be forbidden.



Synthetic order data. The model never calls the external service directly. This is not a universal provider message format.

Request

The model proposes a tool name and arguments.

Boundary

The application validates the shape and authorizes using its trusted session identity.

Result

The application returns a result or error as context, associated with the request ID.

↗ **The model proposes a tool name and arguments.**

PUT IT TO WORK

An own-order lookup may run. A schema-valid lookup for someone else must be refused by application authorization.

CLOSE THE PAGE. EXPLAIN IT.

What must your code check that a schema alone cannot establish?