Corresponding essay: **E09** “Tools Give Models Hands”

PERMISSIONS TRIANGLE

Permissions Triangle

Bring one real tool an agent can already call. Score its three corners 0 to 3, then write one row of the tool registry.

BRING one tool the agent can already call. _____

Step 1 - Score the three corners

Scope: 0 read-only, 1 single resource, 2 multiple resources or one tenant, 3 production or account-wide. Reversibility: 0 no state change, 1 automatic undo, 2 manual but reliable rollback, 3 no dependable undo. Observability: 0 visible on preflight, 1 immediate alert, 2 sampled or delayed review, 3 discovered only after harm.

Criterion	Score (0-3)	Evidence
Scope - how far the action can reach if called wrongly	0 1 2 3	
Reversibility - how hard the action is to undo	0 1 2 3	
Observability - who outside the agent sees it in time to act	0 1 2 3	

Step 2 - Defend the worst corner first

Whichever score is highest is the corner to defend first. Tick the move that applies.

- ☐ Scope is worst: shrink the authority - issue a short-lived, task-bound credential, not an account-wide token.
- ☐ Reversibility is worst: move the point of no return further away - gate the destructive path, add a delayed delete.
- ☐ Observability is worst: build an action ledger and alerts the agent cannot edit; show a preflight plan before any apply.
- ☐ A 3 on any corner: do not let the agent run this tool unattended until the corner is brought down.

Step 3 - Write the tool-registry row

One row per tool. Three threes and an empty owner column is the incident, on one line, before it happens.

Tool	Action class (read / write / destroy)	Scope (0-3)	Reversibility (0-3)	Observability (0-3)	Owner	Default rung (unattended?)	Kill switch

Companion worksheet to **Essay 09 · Tools Give Models Hands**, in the series **Architecting the AI Coworker**. · Dr Peter McCann Strain · Fill this in against one real agent, action class or vendor. © 2026 Peter McCann Strain.

Series Companion + all 22 worksheets: **Release_v12/Series_Companion.pdf**