

Tool and Harness Design Review

Use this checklist in your next design review. Tick each statement that is true for your agent today. Thresholds and intervals in the guide are recommended starting points; calibrate to your environment.

INVENTORY AND TIERS

- ☐ Every tool is listed and assigned a risk tier (read-only, reversible write, irreversible or external write).
- ☐ Any tool whose tier is unclear is treated as Tier 3 until it is classified.
- ☐ Read and write actions are separate tools.
- ☐ Tools expose only the actions the agent needs, not a whole API.

TOOL CONTRACTS

- ☐ Each tool description states when to use it and when not to use it.
- ☐ Input schemas are strict, with enumerated values instead of free text where possible.
- ☐ Long outputs are summarised by the tool and the full output is stored elsewhere.

HARNESS CONTROLS

- ☐ Tier 2 and Tier 3 tools use idempotency keys.
- ☐ The harness, not the model, controls retries for state-changing actions.
- ☐ Timeouts and a maximum number of calls per run are set.
- ☐ Permission scope and approval rules are checked before every execution.

OPERATIONS

- ☐ Success rate and error types are measured for each tool.
- ☐ A repeated-call test confirms no duplicate side effects.
- ☐ Every Tier 3 tool has a signed-off go or no-go decision.

Score: ____ of 14. Any unticked box is a gap to close before the agent handles real work.

Full guide: readyforrole.com/blog/tool-design-harness-engineering.html | Series hub:
readyforrole.com/blog/enterprise-ai-agent-engineering.html | support@readyforrole.com