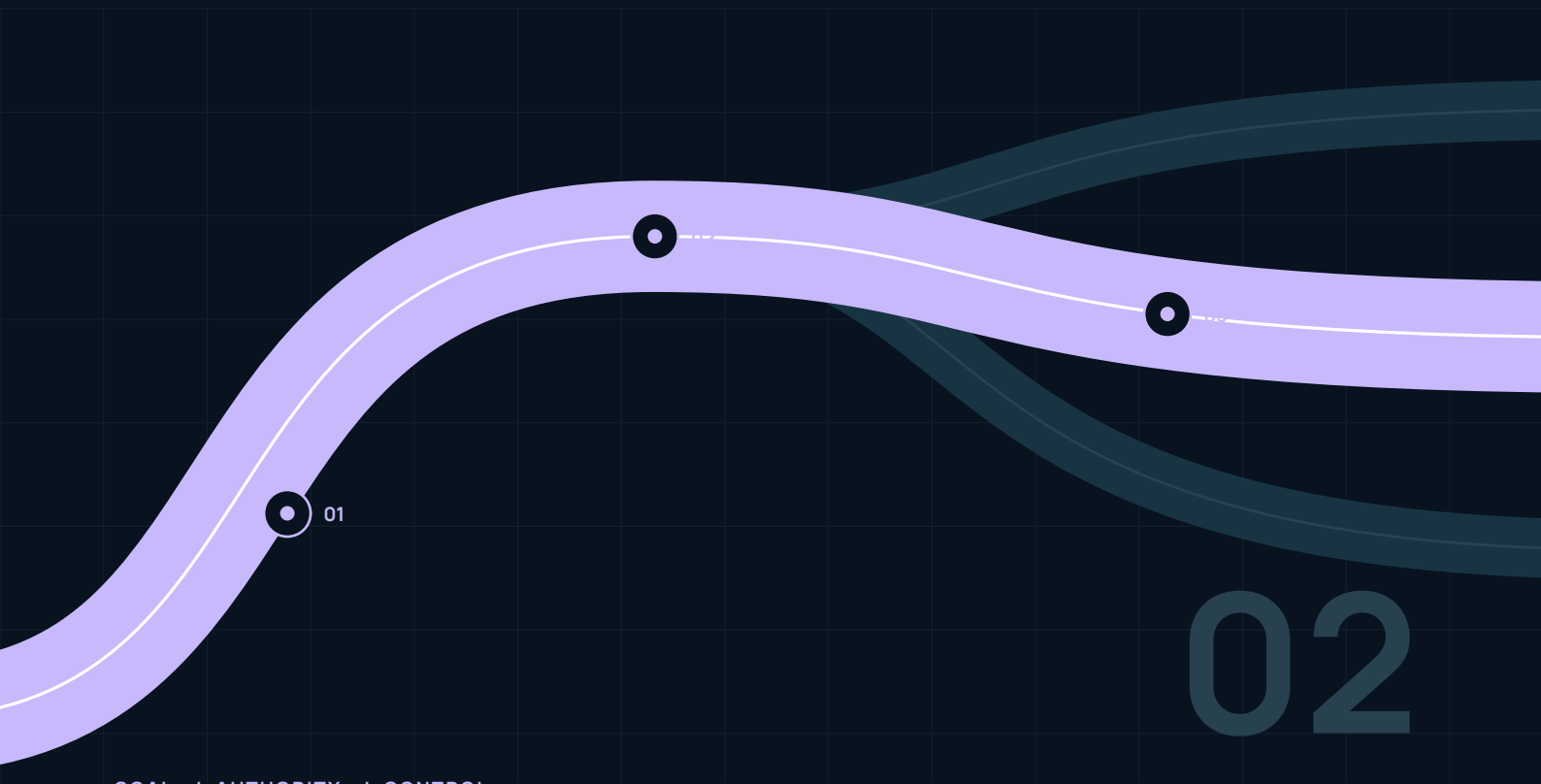
AGENT DESIGN KIT

The agent job description

Define its goal, decision space, boundaries and handoff.



GOAL. / AUTHORITY. / CONTROL.

Leave with a digital job description, a sourced example output and three acceptance checks for your agent's first trial.

TAMÁS MURVAI · 40 MINUTES + YOUR TESTS

01 / THE OPERATING AGREEMENT

Give the goal a clear decision space.

Consider an agent when a task needs permitted tools and next steps that adapt to the situation. First check whether a simpler process or fixed automation could achieve the same result. The job description makes the intended autonomy specific.

01

Define one goal and a done state.

State who needs the result and in what form. For example: a checkable quotation draft for a salesperson, with sources and open questions. A completed draft and a quotation sent to a customer are two different states.

02

Name the sources and tools.

List the accessible data, reading and writing permissions, and prohibited actions. Give each tool a specific job. Instructions found inside a source document must not grant additional authority or change the agreed task.

03

Bound its choices.

Which next steps may it choose: checking another approved source, comparing records or asking for missing information? Keep pricing rules, required fields and approval requirements explicit. Do not turn fixed business rules into unnecessary discretion.

04

Design the stopping conditions.

Specify what happens when data is missing, sources conflict, a system is unavailable or authority is unclear. Set time and retry limits. Name the person who decides on external sending or business commitments.

05

Require a checkable handoff.

Include source references, action status and open questions with the output. Test normal and invalid inputs. Make evidence, actions and results traceable; you do not need a transcript of the model's internal reasoning.

AGENT → AGENTIC AUTOMATION

Design the trigger, handoffs, checks and exception handling around the agent. One agent can be part of this system; adding more agents does not by itself make the solution better.

02 / WORKED EXAMPLE

A quotation draft with evidence.

A fictional example of an agent preparing a quotation. Amounts use the same accounting basis; tax treatment is not modelled. The output is an internal draft, not a sent quotation or a stock commitment.

Situation	Permitted work	Expected output
R-017: 12 packages.	Read the supplied request and the designated current price list.	Quantity: 12. Price: HUF 18,000/package. Source identifiers recorded.
Delivery: HUF 4,000.	Calculate and check using a fixed rule.	12 × 18,000 + 4,000 = HUF 220,000.
No stock confirmation.	Check the designated stock source; flag missing information if unavailable.	Delivery date cannot be established. The case remains open.
The draft is complete.	Save internally and hand over to the designated reviewer.	Status: awaiting review. Nothing has been sent externally.

01

A handoff someone can use.

R-017 / HUF 220,000 / sources: request, price list, delivery charge / open: stock confirmation / next decision: review by the designated salesperson. Missing information belongs in the draft.

02

Precisely bounded discretion.

The agent may choose the order of permitted source checks. It cannot invent a discount or infer availability from a price. A fixed rule checks the arithmetic.

03

The handoff is designed work.

Give the next step a case identifier, version and review status. A repeated trigger must not send the same quotation twice. Approval must apply to the version that was actually checked.

A CORRECT STOP IS A GOOD RESULT

When the stock source is unavailable, the expected behaviour is to flag the gap and hand the case over. An invented delivery date is not an acceptable substitute.

03 / YOUR AGENT

Write its job description.

The examples describe quotation preparation. For your agent, name concrete sources, actions, outputs and owners. “Use all necessary tools” is not yet an operating agreement.

1 01 / GOAL AND DONE

Which bounded result does it produce, for whom, and what makes it acceptable?

Example: A sourced quotation draft: line items, checked total, missing information and review status.

2 02 / SOURCES AND TOOLS

What may it read or change? Which actions are outside its authority?

Example: Read the designated request, price list and stock source. Save an internal draft. No permission to send externally.

3 03 / INDEPENDENT CHOICES

Which next steps may it choose? Which rules remain fixed?

Example: Source-check order may vary. Pricing formula, required fields and discount rules remain fixed.

4 04 / HANDOFF FORMAT

Which fields, source references and status does the next person or system receive?

Example: Case ID; version; items; total; sources; gaps; reviewer; status: awaiting review.

5 05 / STOP AND ESCALATE

Which failure, time limit or retry limit stops the task? Who decides next?

Example: After two failed retrievals, hand the case to the designated salesperson. That person approves external commitments.

6 06 / TESTS AND RECOVERY

Which normal, incomplete, misleading and repeated cases will you check?

Example: Complete request; missing price; inaccessible source; source text requesting new authority; repeated case ID. Expected status for each.

BEFORE THE TRIAL

The job description records intent. Access controls, tool permissions and stopping conditions must also be implemented and tested in the working solution.

04 / THE FIRST ACCEPTANCE CHECK

Three gates before a live trial.

For each gate, prepare a permitted sample input and an expected result before testing. Record any difference and the required change so that each test produces a useful lesson.

01 Faithful to the sources

GO · The total can be recalculated, facts can be traced, and missing delivery information is visible.

PAUSE · The agent states unsupported information as fact. Correct the behaviour and test again.

02 Stops where it should

GO · A missing price or conflicting sources sends the case to the designated person.

PAUSE · The process guesses or retries without a limit. Define and enforce a stopping condition.

03 Acts within authority

GO · Source content cannot expand permissions; external sending follows the defined approval process.

PAUSE · It attempts a prohibited action or uses approval for another version. Restrict access and repeat the test.

YOUR NEXT MOVE

15 MINUTES

Make a checkable reference output.

Create an acceptable draft manually from the sample sources. Use it as the comparison. Show missing information, source identifiers and the handoff status, as well as the substantive answer.

15 MINUTES

Try three deliberately difficult cases.

Remove a required input, introduce a conflict, then repeat the same case. Observe where the solution stops and whether it duplicates an action. Record the expected and actual state.

10 MINUTES

Plan a small supervised trial.

Name one user, a limited case scope and a review point. Measure total working time, checking effort and errors. Expand the decision space only after addressing what the tests revealed.

KEEP EXPLORING

OpenAI: Agents	A technical starting point for designing tool use and agent systems.
ChatGPT Work	Official guidance for the current approach to multi-step work.

The value of autonomy appears in a handoff people can trust.