

01 / DEFINE THE DECISION

Start with one consequential action

Choose a workflow that changes a business record or commits an action outside the conversation. Work through one ordinary request and one exception before discussing how many agents it needs.

A procurement exception to examine

Hypothetical example: a procurement assistant prepares an order for 40 laptops. A manager approves the supplier, quantity, price and delivery location. A revised quote then names a different supplier and raises the total. The team must decide where that change is held, who reviews it, and what evidence confirms the eventual order.

Keep the original map visible

Intent → Authority check → Tool action → Evidence. State the requested result, check who may authorize the particular action, execute within that authority, then inspect what happened at the destination. A useful proposal and a completed business action are different outcomes.

Ask the three questions

Which identity and scope authorize this action? Where is approval checked before execution? What result and audit evidence must be retained? Keep these questions attached to the workflow as it moves between people and systems.

WORKING NOTES

Workflow and consequential action

Name one action, its destination and the person accountable for the outcome.

What counts as a completed result?

Describe the destination evidence, not just the assistant reply or an accepted request.

Exception to test first

Use a changed supplier, amount or recipient that must trigger a new decision.

02 / ROUTING AND INFORMATION BOUNDARIES

Choose the workflow, then the agents

Use the least complicated arrangement that can complete the work and explain its decisions. More agents introduce handoffs, context transfers and failure paths that someone must own.

Make every handoff explicit

For each step, name the initiating user, coordinator, tool or specialist, destination and accountable owner. Specify its inputs, expected output, next step and stop condition. A coordinator can route work; that role does not create authority for the receiving service.

Carry relevant context, not unrestricted access

Identify the quote, budget, supplier record and policy version needed for this order. Decide which records each participant may read, what may cross organizational or hosting boundaries, and what must be redacted. Treat supplier documents and tool output as information to assess, not instructions that can grant permissions.

Arrangement	Use when	Question to settle
Defined workflow	Steps and rules are stable.	Can ordinary software handle the sequence?
Single coordinator	The path varies within a bounded task.	Which routing choices need an explicit limit?
Specialist handoffs	Distinct capabilities justify separate roles.	Who owns context and the returned result?
Human-led exception	Evidence or authority is unresolved.	Who receives the case and decides the next step?

WORKING NOTES

Selected arrangement and reason

Explain why this workflow needs its proposed coordination or specialist roles.

Information and handoff boundaries

Record permitted sources, recipients, sensitive fields and an owner for each handoff.

03 / AUTHORITY BEFORE EXECUTION

Keep approval attached to the action

MCP connectivity, a working credential and a manager's purchase approval answer different questions. Make the application and connected services check the distinctions.

Separate connection from business permission

MCP standardizes interaction between compatible clients and servers. Its authorization specification covers HTTP transport access; that does not decide whether this manager may approve this purchase. Record the acting identity, tool scope and independent business authority. Do not let a model, retrieved document or successful connection supply missing approval.

Approve a particular proposal

Define the details that approval covers: supplier, quantity, amount and currency, delivery destination, operation and relevant policy or quote versions. Give the approver these details in an understandable form. Set an expiry and an accountable owner for exceptions. Assign an owner who can revoke approval and define the review for a changed proposal.

Revalidate at the execution boundary

Require the executing service to check current identity, permissions and the approval for the submitted details before a consequential action. A changed supplier, amount, destination or material policy version should return the proposal for the appropriate new decision. Test expired approval and revoked access, including a change made after approval but before execution.

WORKING NOTES

Approval owner and permitted scope

State who can approve which action, amount and destination, and where that rule is checked.

Approved details and expiry

List the proposal and source versions covered, the validity period and material-change triggers.

Execution-time check and failure response

Name the enforcing service and what happens if approval is missing, changed, expired or revoked.

04 / FAILURE, RECONCILIATION AND INTERVENTION

Handle uncertainty before another attempt

A timeout says that a response was not received. It does not establish that the purchase order was never created. Keep uncertain outcomes visible until they are resolved.

Retain an action receipt

Keep a request identifier, acting identity, proposal and approval references, requested operation, authorization decision, destination identifier, result and any human intervention. Restrict evidence access and retention; keep credentials and unnecessary personal data out of the receipt.

Make recovery a business decision

Before retrying an uncertain write, reconcile with the destination. Use a stable request identifier and idempotency only where the destination actually supports and enforces the intended semantics and retention window. Otherwise stop for investigation. Define a human owner, escalation deadline and permitted recovery action. Cancellation or a compensating transaction may require fresh approval; a rollback is not always available.

Observed state	Next action
Confirmed completion	Retain the destination record and matching receipt.
Denied or changed proposal	Hold execution; explain the review required.
Timeout or lost response	Mark outcome unknown; reconcile before another write.
Partial multi-step result	Stop dependent work; route the evidence to the recovery owner.

WORKING NOTES

How will an unknown result be reconciled?

Name the destination lookup, request identity and person who resolves ambiguity.

Escalation, cancellation and recovery

Record time limits, the decision owner and which recovery actions require approval.

05 / EVIDENCE FOR A RELEASE DECISION

Pilot against outcomes and full cost

Agree on acceptance before running the pilot. Use authorized test identities and synthetic records, with observers able to inspect what reached the destination.

Set limits for the whole workflow

Choose spending, tool-call, retry, elapsed-time and human-review limits, with a named enforcement point and stop owner. A prompt asking an agent to stay within budget is not the same as an enforced limit. Budget exhaustion or missing evidence should produce a visible unresolved case, not a fabricated completion.

Count the cost of an accepted result

Include model calls, retrieval, tools, infrastructure, retries, monitoring, human review, exception handling and an allocated share of setup and maintenance for a stated period. Divide by accepted completed tasks, not attempts or tokens alone. Compare against the current workflow using equivalent quality and risk requirements.

Keep the acceptance record

For unchanged approved details, require one confirmed purchase order with a matching receipt. Changed details must stay held for the appropriate new decision. Test expired approval, revoked access and a lost response after creation, including duplicate handling. Retain test cases, versions, approvals, logs, observations and failed or unobserved paths. Lack of destination visibility is missing evidence, not a pass.

Choose the next step

Record proceed, revise or stop with an accountable owner and review date. Define who can pause the workflow and how an incident or changed dependency reopens the decision. Recheck the release decision when scope, permissions or dependencies change.

WORKING NOTES

Pilot limits and stop owner

Set workflow budgets and the person authorized to stop the exercise or deployment.

Acceptance evidence and unresolved paths

Specify required successful and denied cases, destination checks and evidence still missing.

Decision, accountable owner and review date

Proceed, revise or stop. Record the reason, full cost per accepted result and next review.