



Tool Registry Planning Template

A worksheet for defining read tools, write tools, approval-gated tools, schemas, permissions, fallbacks, and receipts.

STRUCTURE - CLARITY - BETTER DECISIONS

Practical architecture for accountable AI-enabled work.

What this template is for

Give agentic workflows a deterministic operating layer so tools carry state, permissions, validation, execution, and evidence. Use this guide to make the operating choice explicit, test it with evidence, and record who owns the next decision.

BEST USED WHEN

Teams turning architecture work into a reusable operating artifact.

WHO SHOULD BE IN THE ROOM

Include the workflow owner, a person who performs the work, a reviewer with authority to approve or stop it, and the relevant data or tool owner.

CANADIAN CONTEXT

Confirm applicable federal, provincial, territorial, sector, professional, contractual, accessibility, and bilingual-service requirements. Use this workbook as operational preparation, not legal advice.

A five-step working rhythm

01

Read tool

What state can the system retrieve safely?

02

Write tool

What state can the system change, create, send, or assign?

03

Validation

What schema, permission, or business rule must pass first?

04

Approval

Which actions need human approval before execution?

05

Receipt

What result proves the tool completed correctly?

Build the working record

Complete one record for one workflow. Write enough to support a decision, not a generic technology wish list.

PROMPT	YOUR WORKING NOTES
01 Workflow supported	
02 Systems involved	
03 Highest-risk write action	
04 Read tool	
05 Write tool	
06 Validation	
07 Decision, owner, evidence, and review date	

Register document retrieval

STARTING FRICTION

An assistant needs files from the active engagement but must never browse another client workspace.

WORKFLOW MAP



AI-SUPPORTED ROLE

Choose only approved tools, pass validated inputs, and attach execution receipts to the workflow. Flag uncertainty around read tool.

HUMAN AUTHORITY

Tool owners set permissions, test failure modes, and approve consequential writes. Resolve the read tool question for this case.

PILOT MEASURE

Count rejected calls, tool failures, unlogged actions, retries, and permission changes. Record read tool exceptions separately.

DISCUSSION PROMPT

What evidence would the reviewer need to trust, correct, reject, or escalate this output?

Register stock and supplier tools

STARTING FRICTION

Read-only stock checks and purchase-order submission need different authority.

WORKFLOW MAP



AI-SUPPORTED ROLE

Choose only approved tools, pass validated inputs, and attach execution receipts to the workflow. Flag uncertainty around write tool.

HUMAN AUTHORITY

Tool owners set permissions, test failure modes, and approve consequential writes. Resolve the write tool question for this case.

PILOT MEASURE

Count rejected calls, tool failures, unlogged actions, retries, and permission changes. Record write tool exceptions separately.

DISCUSSION PROMPT

What evidence would the reviewer need to trust, correct, reject, or escalate this output?

Register calculation tools

STARTING FRICTION

A model should call a verified calculation service rather than improvise arithmetic in prose.

WORKFLOW MAP

TOOL NEED

CONTRACT

PERMISSION

TEST CALL

APPROVAL

RECEIPT

AI-SUPPORTED ROLE

Choose only approved tools, pass validated inputs, and attach execution receipts to the workflow. Flag uncertainty around validation.

HUMAN AUTHORITY

Tool owners set permissions, test failure modes, and approve consequential writes. Resolve the validation question for this case.

PILOT MEASURE

Count rejected calls, tool failures, unlogged actions, retries, and permission changes. Record validation exceptions separately.

DISCUSSION PROMPT

What evidence would the reviewer need to trust, correct, reject, or escalate this output?

Before the pilot grows

Use these prompts to test whether the proposed workflow can operate responsibly in its Canadian business context.

01

Read tool

Read tools are separated from write tools. Name the owner and the operating decision before selecting a tool.

02

Write tool

Every tool has a typed input and structured output. Record the approved sources, permissions, and missing information.

03

Validation

Permissions are checked before execution. Test this boundary with representative and adverse cases.

04

Approval

High-risk writes require approval preview. Preserve review, escalation, and correction evidence.

05

Receipt

Tool failures create visible fallback or retry paths. Set a measurable stop condition and the next review date.

06

Readiness to proceed

A tool registry is where agentic systems become operational. Without tool contracts, agents improvise around business state.

CANADIAN REFERENCE POINTS

Office of the Privacy Commissioner of Canada - Privacy and artificial intelligence
priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/

Government of Canada - Artificial Intelligence guidance, principles, and policy
canada.ca/en/services/science/innovation/artificial-intelligence.html

General operational guidance only. Confirm applicable legal, privacy, cybersecurity, professional, contractual, and regulatory requirements with qualified advisors.