

AGENT AUTHORITY REGISTER

A working record of who authorized an AI agent to do what, against which resource, with what evidence, and until when.

HOW TO USE IT

- 1 Pick one production agent**

Start with an agent that can touch code, identity, infrastructure, customer data, money, or another consequential resource.
- 2 Record delegated authority**

Name the accountable owner and the person or system that delegated the authority. Do not treat authentication alone as approval.
- 3 Attach evidence**

Reference the system of record, ticket, policy, approval, contract, configuration, or other evidence that supports the authority claim.
- 4 Set current state**

Mark authority Authorized, Step-up, Unresolved, or Revoked. A blank or unsupported cell is unresolved authority, not implied approval.
- 5 Set the next review**

Record the review or expiry date and the next action required. Revisit the row when the scope, owner, resource, agent, or authority changes.

WEEKLY COMPLETION TEST

One production agent has a named accountable owner, a named delegator, a bounded action and resource, evidence supporting the authority, a current authority state, and a review or expiry date.

BOUNDARIES

- This workbook is an operating record, not a compliance certification or automated authorization system.
- Keep facts and inferences separate. Use Claim Status to distinguish verified evidence from assertion, inference, missing evidence, or conflict.
- Reference existing systems of record rather than copying sensitive evidence into this workbook when a pointer is sufficient.

SOURCE NOTES

NIST, Comments on Software and Agentic AI Identity Concept Paper (Sep. 29, 2026): <https://www.nist.gov/news-events/news/2026/09/comments-software-and-agentic-ai-identity-concept-paper>

IETF WIMSE, AI Identity Management System draft-ietf-wimse-aims-00 (Sep. 15, 2026): <https://www.ietf.org/archive/id/draft-ietf-wimse-aims-00.html>

EXAMPLE ONLY

Agent	Owner	Delegated by	Action	Resource	Evidence	State	Review
CI deployment	VP Engineering	Release manager	Deploy approved build	Staging environment	Approved change ticket	Authorized	End of release window