GOVERNANCE DOCUMENT

AGENT AUTHORIZATION RECORD

sougataroy.com

No platform ships this record. Complete one per deployed agent before first execution. This document answers the question the audit trail cannot: who formally decided what this agent is authorized to do, and whose name is on that decision.

Agent Authorization Record, v1.5, August 2026. Current version at sougataroy.com/frameworks/agent-authorization-document

01, IDENTIFICATION

AGENT NAME

The display name used in the agent registry, admin center, or internal inventory.

BUSINESS PURPOSE

One to three sentences explaining the problem this agent solves and the workflow it supports.

02, AUTHORIZATION SCOPE

AUTHORIZED ACTIONS

List each action the agent is permitted to take, using precise language tied to specific systems or workflows.

EXPLICIT PROHIBITIONS

List what the agent must not do. If this field is blank, the authorization record is incomplete.

DATA ACCESS SCOPE

Name the systems, libraries, sites, datasets, or applications the agent can read from and write to.

AGENT AUTHORIZATION RECORD

03, ACCOUNTABILITY

BUSINESS SPONSOR

Full name and title of the named human the organization maps from the Sponsor role in Microsoft Entra Agent ID. The platform Sponsor can be a user or supported group accountable for purpose, lifecycle decisions, and access reviews; this record requires one named accountable human for the business authorization decision.

TECHNICAL OWNER

Full name and title of the administrator responsible for this agent's operational management, permissions, and identity configuration. Maps to the Owner role in Microsoft Entra Agent ID. Not the approving authority.

04, REVIEW AND APPROVAL

REVIEW TRIGGER CONDITIONS

Describe the events that require re-authorization, such as a change in purpose, data access, ownership, regulation, or an incident.

NEXT SCHEDULED REVIEW DATE

Set the date when the organization will confirm the record is still accurate and complete.

AUTHORIZATION SIGNATURE

Capture the approving person's name, title, and date. This should be the accountable business owner, not only the developer or IT administrator.

05, STANDING TRIGGERS

An agent that runs on a schedule was authorized once. The schedule that wakes it was not.

Most authorization records approve an agent and stop there. When that agent runs unattended on a timer, a cron schedule, or an external event, a second decision exists and is almost never written down: who decided the run should happen, why it must happen without a person present, and when anyone will ask whether it still should. Complete this section once per standing trigger attached to the agent.

TRIGGER DEFINITION

The timer, schedule, or external event that starts an unattended run, recorded in the form the platform stores it, together with the action it starts.

CONSEQUENCE OWNER

Full name and title of the person accountable for what the unattended runs cause. Distinct from the Technical Owner who configured the trigger and from the Business Sponsor who approved the agent.

GOVERNANCE DOCUMENT

AGENT AUTHORIZATION RECORD

sougataroy.com

ACTIVATION JUSTIFICATION

One sentence stating why this run must occur without a person present, and what fails if it does not.

TRIGGER REVIEW DATE

The date the organization will confirm the run still needs to exist. Separate from the agent's Next Scheduled Review Date, because an agent can remain justified while a schedule attached to it no longer is.

TWO OPERATING RULES

Orphaned triggers. A standing trigger whose Consequence Owner has left the organization is treated as an unauthorized deployment from the date of departure, suspended until a new owner signs. Reassigning the agent does not carry the trigger. Authority to run and authority to begin running are separate grants, and this section records the second one.

Offboarding. The offboarding checklist lists every standing trigger the departing person configured and reassigns each by name before final-day access is removed. A trigger that reaches the departure date unassigned is suspended, not inherited.

LIMITATION

This section records who authorized a run to begin and when that authorization expires. It cannot prove the run still serves the purpose stated, and it does not surface triggers the organization has never enumerated.

The standing trigger clause was introduced in The Governance Gap, "The Agent Was Authorized. The Schedule Never Was.", August 11, 2026. sougataroy.com/newsletter/agent-authorized-schedule-never-was

This template is informed by accountability and oversight expectations in NIST AI RMF, OMB M-25-21, FINRA's 2026 Regulatory Oversight Report, and Article 26 of the EU AI Act. Field labels map to role definitions in Microsoft Entra Agent ID. Free to use and adapt with attribution to Sougata Roy and sougataroy.com. No gate. No form.