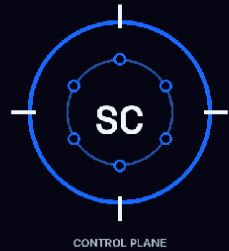


SESSION CUSTODY

EXPLAINER SERIES



CATEGORY EXPLAINER

What Is an Agent Governance Control Plane?

A clear definition of the infrastructure layer for governing autonomous work in motion.

GOVERN • CONTROL • ENFORCE



GOVERN THE SESSION, NOT THE REQUEST.

sessioncustody.ai

Publication Edition | Explainer 02 | April 16, 2026

EXPLAINER 02 | APRIL 16, 2026 | THE CATEGORY

What Is an Agent Governance Control Plane?

A clear definition of the infrastructure layer for governing autonomous work in motion.

The Control Layer for Autonomous Work

An Agent Governance Control Plane, or AGCP, is a vendor-neutral infrastructure layer for governing autonomous enterprise work while that work is happening. It is designed for agents that do more than generate answers - agents that call tools, update workflows, consume resources, delegate subtasks, and create side effects in systems of consequence.

The AGCP makes that activity governable as sessions. A governed session is the complete chain from objective through planning, policy context, approvals, tool use, retries, delegation, containment, termination, and evidence. A request is a moment. A session is the unit in which enterprise authority and accountability continue across time.

An AGCP answers a current-state question: should this proposed consequential action proceed now, in this session, under this authority, with this policy state, delegated lineage, revocation posture, economic boundary, and enforcement coverage?

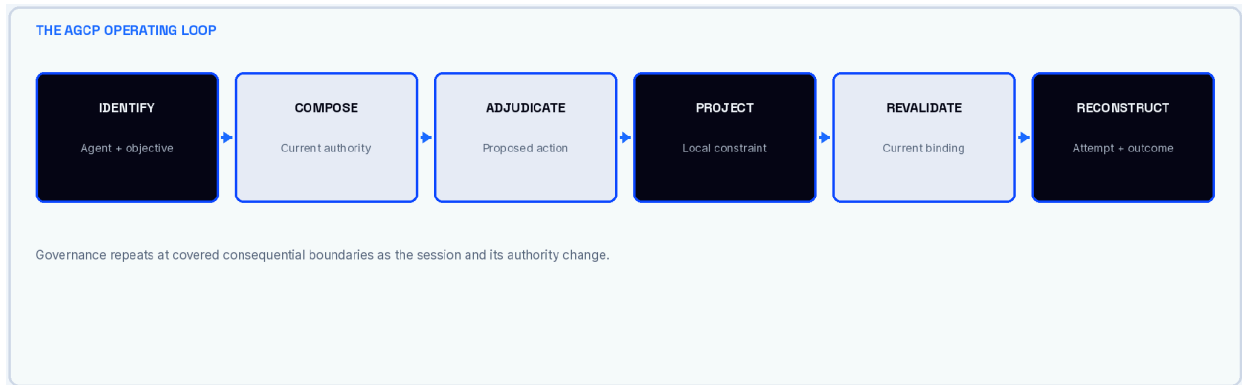


Figure 1. An AGCP maintains a current session-level control loop across heterogeneous sources, runtimes, and systems of consequence.

Where the AGCP Sits

Systems of record remain authoritative for native facts such as identity, policy, approvals, workflow commitments, cost, incidents, and target outcomes. Agent runtimes, gateways, brokers, wrappers, and target adapters remain responsible for the local mechanics they can enforce. The AGCP maintains the cross-system session-level relationships needed to decide and preserve authority across those boundaries.

For supported sources, authenticated interfaces present applicable authority facts in maintained normalized representations with source, version, freshness, integrity, and lineage. The control plane forms the current effective-policy object for the governed session, binds decisions to that policy state and the current session snapshot, and projects supported constraints to covered enforcement points. A local projection does not become an independent or permanent source of authority.

What an AGCP Is Not

An AGCP is not a chatbot, model router, prompt filter, approval queue, trace viewer, generic governance dashboard, or runtime sandbox. Those systems can remain essential. Their role is different.

- A **model gateway** can route and filter model traffic; it does not by itself maintain the authority-bearing state of a complete autonomous session.
- An **identity platform** can establish principal and credential state; identity alone does not define objective, approval scope, or current delegated authority.
- A **GRC or workflow system** can hold policy and approval records; those records become operational only when their applicable scope and current state affect the proposed action.
- A **runtime security control** can enforce local restrictions; local enforcement does not by itself resolve cross-system session authority.
- An **observability platform** can reconstruct events; observation alone does not decide whether the next covered consequence should occur.

The Six Linked Functions

Principle	Operational question	Control-plane responsibility
GOVERN	Who owns this work, and what may it accomplish?	Bind the agent and session to identity, owner, objective, approved purpose, scope, authority ceiling, and stop conditions.
CONTROL	Is the work still aligned as conditions change?	Maintain current session state and refresh decision context when material policy, approval, trust, economic, or containment state changes.
ENFORCE	Should the next covered consequence occur?	Adjudicate the proposed side effect and project supported local constraints to a mandatory enforcement path.
DELEGATE	Did downstream work inherit the right limits?	Carry child objective, authority ceiling, policy binding, budget, exception scope, lineage, and revocation reference.
CONTAIN	Can changed authority reach active work?	Advance control state and fence affected sessions before the next covered consequence.
RECONSTRUCT	Can the enterprise explain decision and outcome?	Link objective, policy lineage, decision, enforcement, attempt, target result, rationale, and accountability.

The Technical Center

The category becomes concrete through an ordered relationship among machine-maintained state, pre-consequence decision, local enforcement, downstream revalidation, and outcome correlation. The system maintains current session authority, evaluates a typed proposed action, returns an operational result and rationale, projects supported constraints from the same governing policy state, and prevents covered execution under a stale or mismatched binding.

Delegation uses the same principle. A child can execute locally, but its downstream constraint bundle remains bounded by the parent authority ceiling and carries current policy and revocation references. Before a covered consequential action, the action fence verifies that the decision or bundle remains current. Changed authority can therefore affect already-active work rather than only future session starts.

Why the Category Matters

Autonomous agents become enterprise infrastructure only when their work can be attributed, evaluated against current policy, interrupted when authority changes, bounded by economic conditions, and reconstructed from objective through actual outcome. The AGCP supplies the continuing control relationship that lets existing enterprise systems contribute their native strengths without requiring one of them to own the entire session.

An AGCP does not centralize every reasoning step. It preserves enterprise authority at the transitions where autonomous intent can become enterprise consequence.

OPERATING BOUNDARY

These explainers describe the Session Custody product and category at a conceptual and operational level. Coverage depends on supported sources, configured mappings, authenticated integrations, and declared enforcement paths. The architecture does not assume a universal policy language, permanent authorization, human approval for every action, or replacement of the systems that own native enterprise facts and outcomes.