

Delegated Authority Across Buyer and Provider Agents

An Executive Mandate for Identity and Action

Phil Hatch | Akholi

October 23, 2026

The buyer should approve a bounded grant of business authority for every outsourced agent. That grant must survive tool use, further delegation, configuration change, and revocation across both organizations.

Approve the Authority Being Delegated

The executive sponsor should approve the business authority of an outsourced agent separately from the decision to buy the service. Access to a tool does not explain which actions the provider may take on the buyer's behalf. A contract description such as case resolution can conceal materially different powers to read, recommend, amend, commit, or delegate.

The proposed authority mandate records the action, protected resource, permitted purpose, operating conditions, duration, and accountable buyer. It also identifies the provider principal exercising that authority. An agent should receive only the permissions needed for the approved task, with consequential actions enforced by systems that the agent cannot instruct to waive the restriction.

NIST's February 2026 identity initiative identifies authorization, auditing, and non-repudiation as agent-specific design questions. It is a concept-paper initiative, not a mandatory finished

standard. Executives should require their teams to answer those questions for the actual service rather than accept a supplier's general identity claim.¹

Distinguish Business Authority from Technical Access

A hypothetical procurement agent may have technical access to a purchasing system but authority only to prepare orders below an approved threshold for named categories. The executive mandate should state whether it can commit the buyer, change a supplier, or authorize another agent. Technical teams should then translate those decisions into enforceable permissions.

The study's accounts of staff and shared credentials reveal a practical risk: the recorded identity may not identify the actor or the authority used. They are vendor-team reports, not verified access assessments. Their executive implication is to demand a clear link between the approved business task and the identity performing each consequential action.²

A named buyer employee should not become the implied source of every agent action because a provider borrowed that employee's account. Management should provide a supported route for agent identities and escalation when access is delayed. The alternative should be an authorized fallback, with its service and cost implications visible.

Make Further Delegation a Separate Decision

Figure 1 sets out four authority decisions. Permission to perform a task should not automatically include permission to delegate it. The mandate should specify allowed recipients, narrower child permissions, expiry, and the evidence linking every child action to the original grant. A provider must disclose when another firm enters the delivery chain.

The allied agent-security guidance recommends bounded permissions, recorded grant chains, and controls against unapproved delegation. Those recommendations support the design direction; they do not determine what authority a particular enterprise can lawfully delegate. The buyer's business and legal functions must make that decision for the service.³

¹ National Institute of Standards and Technology, "New Concept Paper on Identity and Authority of Software Agents," National Institute of Standards and Technology, February 5, 2026, project status and identification, authorization, auditing, and non-repudiation questions, <https://www.nist.gov/news-events/news/2026/02/new-concept-paper-identity-and-authority-software-agents>.

² Phil Hatch, *Agentic AI Outsourcing at Tier 1 Financial Institutions: Full Study Report*, version 1.8.2 (Akholi, forthcoming manuscript dated November 1, 2026), Part 3, Financial Institution Readiness, sec. 4.1, "Ability to Provision Access and Identities for Agents," indicator C108, <https://doi.org/10.2139/ssrn.7164559>.

³ Australian Signals Directorate's Australian Cyber Security Centre et al., *Careful Adoption of Agentic AI Services* (Australian Signals Directorate, May 1, 2026), "Manage third-party components," "Identity management," "Resilience," and "Human in the loop," <https://www.cyber.gov.au/publication/careful-adoption-of-agentic-ai-services>.

A delegation should fail closed when its parent expires or is revoked, subject to an approved safe-state design. The firms should test whether queued actions, delegated credentials, and external commitments follow the revocation. An executive should receive the residual exposure, including actions that have already become irreversible.

Figure 1. An authority mandate that survives delegation

Decision	Buyer approval	Provider evidence
Grant	Purpose action resource and conditions	Principal and enforced permissions
Delegate	Permitted recipient and narrower scope	Recorded parent and child grants
Change	Reassessment of authority and exposure	Configuration and test comparison
Revoke	Stop and safe-state requirements	Queued and delegated action reconciliation

Author's proposed operating framework. Adapt to the service and applicable jurisdiction; not an empirically validated standard.

Source: Phil Hatch, proposed framework developed for this paper.

Require Evidence Without Demanding Every Internal Detail

The buyer needs enough evidence to establish who acted, under which grant, on what resource, and with what result. It need not obtain every provider prompt or proprietary implementation detail. Define a minimum action record with reliable timestamps, configuration references, authority identifiers, and the downstream state needed for verification.

The study describes agent actions visible only within each firm's tools. This fragmentation matters because a provider log can prove a request was sent while the buyer's system shows a different result. Reconcile both sides for consequential actions rather than treating either party's success flag as the complete record.⁴

The chief information security officer should agree how evidence is protected and shared. Detailed logs can themselves expose personal information, secrets, or privileged business data. Access restrictions and retention should preserve the required accountability without creating an uncontrolled second repository.

⁴ Hatch, *Agentic AI Outsourcing*, Part 2, sec. 5.1, "Agent Actions Visible Only Inside Each Firm's Own Tools."

Govern Change and Local Requirements

Expanding a tool list, changing a resource, or enabling a new delegation route should reopen the authority decision. A model update may also change behavior without changing permissions. Management should require a change assessment that explains whether the approved task, control effectiveness, or potential consequences have changed.

The approval record should include an authority holder who remains accountable when the agent changes. Replacing one model or orchestrator should not silently transfer the power to commit the buyer to a different provider principal. Require a continuity check of the grant, enforcement points, evidence, and revocation path. This is especially important where the service uses several agents but the buyer has approved only one organization and a defined set of actions.

Mayer Brown's governance analysis recommends checkpoints and least privilege for agents. The buyer-provider mandate proposed here adds explicit ownership at the organizational boundary: who can grant authority, who enforces it, who observes actions, and who can withdraw it. These decisions should appear in the operating schedule as well as the technical configuration.⁵

Global operations should use a common authority vocabulary with local legal annexes. EU, UK, Swiss, and US entities can face different constraints on commitments, data use, and oversight. The mandate should identify the legal entity whose authority is exercised rather than assume a group-wide service account represents every entity equally.

Require a Revocation Demonstration Before Expansion

The executive approval should require a demonstration of normal execution, denied excess authority, and revocation during unfinished work. Management should document what stops, what continues, and what requires recovery. A failed revocation test should restrict the affected authority until the two firms can explain and correct the failure.

The executive decision is whether a defined grant can be enforced and withdrawn across the complete service. Approve the smallest authority that supports the business outcome, fund the necessary identity and evidence functions, and expand only when tests support the additional exposure. The mandate should remain accountable to a named buyer executive.

⁵ Arsen Kourinian, "Governance of Agentic Artificial Intelligence Systems," Mayer Brown, February 24, 2026, "Mitigation Measures," <https://www.mayerbrown.com/en/insights/publications/2026/02/governance-of-agentic-artificial-intelligence-systems>.

Evidence and Source Note

The study is a nonrepresentative cross-section of 850 vendor delivery-team respondents on 150 engagements serving Tier 1 financial institutions, collected during January–June 2026. Neither banks nor vendors corroborated the accounts. It establishes reported experience, not causation, legal breach, or market prevalence. Its application here is a mechanism to investigate, not an estimate of conditions in other industries. The author-supplied version 1.8.2 is dated November 1, 2026 and is cited as a forthcoming manuscript consulted October 23, 2026.⁶

This is an analytical decision paper based on the supplied study and selected primary public sources checked through October 23, 2026. The original contribution is a four-part executive authority mandate that connects organizational permission to enforceable agent grants. The proposed method has not been independently validated. Legal requirements depend on the entity, activity, jurisdiction, and effective provisions; supervisory observations, research, and professional commentary have distinct authority.

Bibliography

Australian Signals Directorate's Australian Cyber Security Centre et al.. *Careful Adoption of Agentic AI Services*. Australian Signals Directorate, May 1, 2026. <https://www.cyber.gov.au/publication/careful-adoption-of-agentic-ai-services>.

Hatch, Phil. *Agentic AI Outsourcing at Tier 1 Financial Institutions: Full Study Report*. Version 1.8.2. Akholi. Forthcoming manuscript dated November 1, 2026. Author-supplied manuscript consulted October 23, 2026. <https://doi.org/10.2139/ssrn.7164559>.

Kourinian, Arsen. "Governance of Agentic Artificial Intelligence Systems." Mayer Brown. February 24, 2026. <https://www.mayerbrown.com/en/insights/publications/2026/02/governance-of-agentic-artificial-intelligence-systems>.

National Institute of Standards and Technology. "New Concept Paper on Identity and Authority of Software Agents." National Institute of Standards and Technology. February 5, 2026. <https://www.nist.gov/news-events/news/2026/02/new-concept-paper-identity-and-authority-software-agents>.

⁶ Hatch, *Agentic AI Outsourcing*, Introduction, "Executive Summary" and "Evidentiary Basis and Its Limits."