

Controlling Provider Changes to Agent-Delivered Services

An Executive Mandate for Material Change

Phil Hatch | Akholi

October 23, 2026

Executives should require a joint decision before a provider change materially alters service authority, behavior, evidence, cost, or dependency. A model or tool update can change the purchased service even when the prime contract remains unchanged.

Govern the Service Change Rather Than the Release Label

The executive service owner should define which provider changes require notice, assessment, approval, or restriction. A vendor may call an update routine maintenance while it changes what an agent can do, which data it uses, or how its results are produced. The buyer's decision should follow the consequence of the change rather than the vendor's release category.

Deloitte's multicountry survey discussion identifies governance maturity lagging reported agent adoption.¹ That survey does not establish that a particular release is unsafe. It supports asking whether the buyer's operating governance has kept pace with the provider's ability to change the service.

Start with the approved service baseline: purpose, actions, data, model, tools, permissions, human roles, evidence, and dependencies. Without that baseline, management cannot explain what changed or determine which earlier acceptance results remain relevant.

¹ Andy Bayiates, "Business and IT Leaders Report AI Agents Are Scaling Faster Than Their Guardrails," Deloitte Insights, April 24, 2026, survey scope and governance discussion, <https://www.deloitte.com/us/en/insights/topics/emerging-technologies/ai-agents-scaling-faster.html>.

Define Materiality in Operating Terms

A change is potentially material when it expands authority, affects a consequential decision, changes the required human judgment, alters data use, weakens evidence, or changes the economics or recovery route. The service owner should define thresholds and require specialist assessment where needed. A small configuration edit can cross a material business boundary.

The study's reports of processes poorly fitted to agents and manual work sustaining delivery identify reasons to assess the whole operating method.² They do not establish the effect of any specific vendor update. The buyer should test whether the proposed change alters its retained work or the assumptions behind its controls.

For a hypothetical support service, enabling a new tool may allow the agent to modify records rather than merely draft advice. The commercial scope and authority decision should be revisited even if the model version is unchanged. Conversely, an update with no material service effect may need a lighter, documented route.

Use a Joint Change Decision Record

Figure 1 proposes four questions: what changed, which approval assumptions are affected, what evidence must be repeated, and who accepts the resulting service. The provider should supply enough information for the buyer to assess those questions before the change reaches material work.

Compare the proposed configuration with the approved baseline. Identify affected workflows, customers, jurisdictions, tool boundaries, evidence, and cost assumptions. Require a test plan tied to the changed mechanism rather than rerun only a general model benchmark. Record limitations where the provider cannot disclose or control an underlying change.

The UK Software Security Code addresses development, maintenance, and supplier communication as parts of resilience.³ The executive application proposed here is a controlled service-change process that preserves security and operating acceptance as the provider's technology evolves.

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 2, "The Shift From Managing People to Managing Agents"; Part 6, "The Executive Action Plan," <https://doi.org/10.2139/ssrn.7164559>; Hatch, *Agentic AI Outsourcing*, Part 5, "The Five Manual Alteration Methods" and "Disclosure of Manual Alteration," table 5.8.

³ UK Department for Science Innovation and Technology, "Software Security Code of Practice," UK Department for Science Innovation and Technology, updated January 15, 2026, voluntary scope and software security and resilience principles, <https://www.gov.uk/government/publications/software-security-code-of-practice/software-security-code-of-practice>.

Figure 1. The material service change decision

Decision area	Executive question	Required record
Change	What can differ in delivery	Baseline and proposed configuration
Impact	Which assumptions no longer hold	Authority data evidence and cost effects
Retest	What must be demonstrated again	Affected acceptance and recovery tests
Acceptance	Who approves the resulting service	Conditions restrictions and closure

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.

Plan for Changes the Buyer Cannot Prevent

Some platform providers may retire a model or deploy an underlying change on terms the prime cannot negotiate. The buyer still needs timely notice where available, impact assessment, substitution options, and a restriction route. Inability to veto the platform does not remove the need to decide whether the resulting service remains acceptable.

The contract should define emergency changes, notice, evidence, rollback or alternative operation, and post-change review. An urgent security correction may need a different approval sequence from a planned expansion, but its service effects and unresolved risks should remain recorded. Emergency treatment should not become a permanent bypass for ordinary change.

EU, UK, Swiss, US, and other obligations may change the required assessment, notification, or approval for a particular activity. Legal, privacy, safety, and risk specialists should identify those conditions. A global maintenance permission should not silently authorize new data purposes or regulated decision roles.

Make the Updated Service Earn Acceptance

A reasonable objection is that joint approval could slow innovation and create repetitive review. Calibrate the route to consequence and reuse unaffected evidence. The purpose is to identify what needs a new decision, not to repeat every original assessment after every technical edit.

The executive should receive material changes, unresolved limitations, retest results, and the effect on business value and retained duties. Require closure evidence for conditions attached to approval. If the provider cannot demonstrate that the changed service remains within the agreed boundary, restrict or substitute the affected function.

The buyer approves an operating service, not a perpetual entitlement for the supplier to redefine it. Controlled change keeps that approval meaningful as models, tools, and dependencies evolve. Expansion should follow current evidence rather than inherit authority from a different configuration.

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, 2026.⁴

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 material service-change decision record linking provider releases to affected authority, evidence, economics, dependencies, and renewed operating acceptance. 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

Bayiates, Andy. “Business and IT Leaders Report AI Agents Are Scaling Faster Than Their Guardrails.” Deloitte Insights. April 24, 2026. <https://www.deloitte.com/us/en/insights/topics/emerging-technologies/ai-agents-scaling-faster.html>.

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>.

UK Department for Science Innovation and Technology. “Software Security Code of Practice.” UK Department for Science Innovation and Technology. Updated January 15, 2026. <https://www.gov.uk/government/publications/software-security-code-of-practice/software-security-code-of-practice>.

⁴ Hatch, *Agentic AI Outsourcing*, Introduction, “Executive Summary” and “Evidentiary Basis and Its Limits.”