

Every Material Provider Update Needs a Joint Acceptance Decision

A Management Method for Change in Live Agentic Services

Phil Hatch | Akholi

October 23, 2026

Managers should classify provider updates by their effect on the accepted service and require joint reassessment where authority, behavior, evidence, or exposure changes. Routine release labels should not determine whether the buyer must accept a changed operating risk.

Assess the Service Effect of the Update

The service manager should ask what changes for the buyer when the provider updates a model, prompt, tool, memory design, interface, or subcontractor. A release described as maintenance can alter permitted actions, output quality, data use, latency, or the evidence available for investigation.

The UK Software Security Code of Practice emphasizes lifecycle maintenance and supplier communication.¹ It is voluntary guidance, not certification. For an outsourced agentic service, the manager should translate relevant lifecycle expectations into a practical notice, assessment, test, and acceptance route.

Identify the currently accepted configuration and the proposed difference. Preserve both. A buyer cannot evaluate the impact of a change if the provider describes only its new capability and cannot establish what was operating before the update.

¹ 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>.

Classify Changes by Consequence

Not every change requires the same review. Define categories for changes within the accepted operating boundary, changes requiring focused retest, and changes requiring renewed authorization. The classification should consider authority, affected population, data, dependencies, human work, and the ability to recover.

The study's reported process and governance-function gaps identify why a static approval can become disconnected from live delivery.² The findings do not establish that every update is unsafe. They support a maintained connection between approved design and actual operation.

For a hypothetical extraction service, a formatting improvement may fit an approved category while adding a tool that writes directly to a customer record changes authority. The manager should assess that difference explicitly rather than apply the same light review because both updates share a release number.

Use a Joint Change Acceptance Record

Figure 1 proposes a record of change, impact, evidence, and decision. The provider supplies the technical and delivery description; the buyer assesses consequences for its obligations and operating model. Record who can approve deployment and what happens if agreement is not reached.

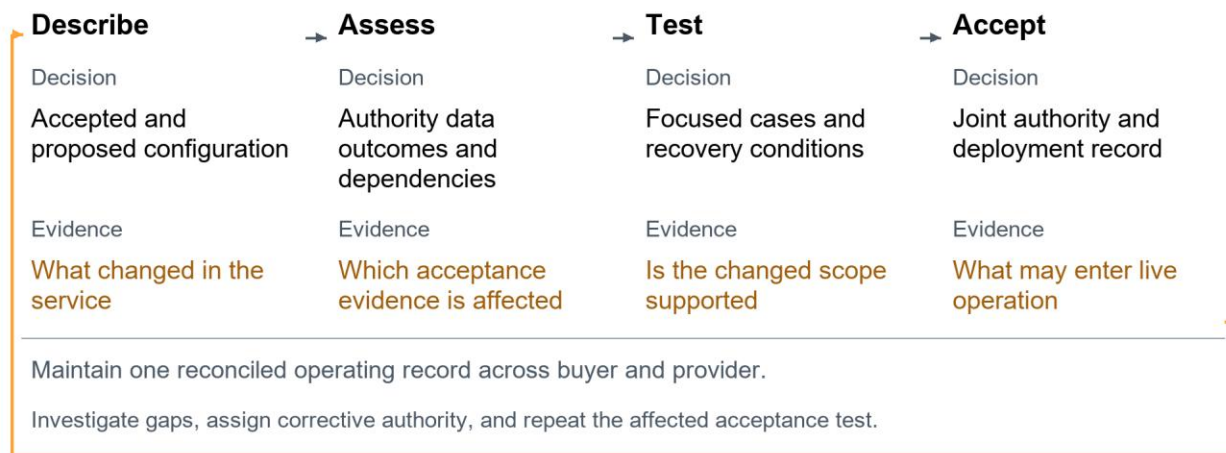
Test affected normal and difficult cases, including human intervention, prohibited actions, and recovery. Reuse valid earlier evidence while identifying the part invalidated by the change. A complete retest may be unnecessary, but the reason for limiting tests should be documented.

Mayer Brown's services-contract analysis emphasizes governance and defined responsibility for agentic delivery.³ Contractual change rights should support the operating decision. Notice alone is inadequate if the buyer receives too little information or has no practical way to restrict an unaccepted update.

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 2, secs. 4.2–4.3, "Human Review Capacity Against Agent Output Volume" and "Routine Approval of Agent Output at Human Review Points."

³ Rohith P. George et al., "Contracting for Agentic AI Solutions: Shifting the Model from SaaS to Services," Mayer Brown, February 17, 2026, secs. 1–6, <https://www.mayerbrown.com/en/insights/publications/2026/02/contracting-for-agentic-ai-solutions-shifting-the-model-from-saas-to-services>.

Figure 1. The joint change acceptance record



Author's proposed method; adapt to the service and applicable jurisdiction.

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

Design for Urgent Changes and Downstream Limits

Security fixes can require rapid action. Agree an emergency route that identifies the risk of delay, temporary restrictions, authorized decision-makers, evidence preserved, and subsequent review. An emergency exception should not become a standing route around ordinary acceptance for unrelated feature changes.

A provider may depend on an upstream model that changes outside its direct control. Require disclosure of that constraint and a plan for affected service behavior. The buyer should know whether version pinning, delayed rollout, restricted operation, or substitution is feasible and at what cost.

EU, UK, Swiss, US, and other contractual, sector, privacy, and regulatory requirements can affect notification and approval. Specialists should establish the local conclusions. Internal change acceptance does not replace any required external authorization, notification, or validation.

Keep the Accepted Service Current

A reasonable objection is that joint acceptance will slow innovation. Pre-agree low-risk categories and evidence standards, automate routine checks where suitable, and reserve specialist decisions for material changes. The aim is a faster informed decision rather than a universal committee meeting.

After deployment, verify the actual version, monitor the affected outcomes, and reconcile pending work. Define rollback or restriction conditions in advance. A rollback should account for actions already taken by the changed service; restoring software does not automatically restore the prior business state.

The manager should maintain a current acceptance history, not a one-time approval file. Each material change should leave an explanation of what changed, what evidence supports it, who accepted it, and how the service remains controlled across the two firms.

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-change acceptance method separating release labels from service consequences and preserving a joint decision history. 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

George, Rohith P., Joe Pennell, Brad L. Peterson, and Oliver Yaros. “Contracting for Agentic AI Solutions: Shifting the Model from SaaS to Services.” Mayer Brown. February 17, 2026.
<https://www.mayerbrown.com/en/insights/publications/2026/02/contracting-for-agentic-ai-solutions-shifting-the-model-from-saas-to-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>.

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.”