

A Vendor Release Can Reopen the Life Sciences Validation Question

A Quality Executive Decision on Changed AI Delivery

Phil Hatch | Akholi

October 23, 2026

Life-sciences executives should require a documented impact assessment when a supplier changes an AI-supported regulated workflow. Prior validation supports the tested use and configuration; it should not be presumed to cover every later model, tool, process, or human-review change.

Ask What the Existing Evidence Still Establishes

The quality executive should identify which accepted claims depend on the supplier configuration being changed. A validation conclusion belongs to a defined context, method, data, system, and operating process. A provider's description of a release as an improvement does not establish that the earlier evidence remains sufficient.

FDA and EMA's joint principles emphasize context-specific assessment and lifecycle management of drug-development AI.¹ They are guiding principles rather than a general validation approval. The organization should determine the actual GxP and local requirements for the affected activity.

For a hypothetical batch-document review service, a model update may change how omissions are classified or evidence is summarized. The manager should assess the effect on the accepted workflow and qualified review, even if the interface and commercial service name remain unchanged.

¹ US Food and Drug Administration and European Medicines Agency, *Guiding Principles of Good AI Practice in Drug Development* (US Food and Drug Administration and European Medicines Agency, January 2026), principles 2, 4–6, 8–10, <https://www.fda.gov/media/189581/download>.

Follow Change Beyond the Model Version

Changes to prompts, retrieval sources, data preparation, thresholds, tool permissions, and human correction can alter the assembled service. The supplier should identify the material differences and dependencies. A version number alone may be insufficient to determine which validation claims are affected.

The study reports governance and process gaps in banking delivery.² It does not establish life-sciences validation failures. The transferable question is whether a changed delivery method still operates within the evidence and controls on which the buyer relies.

Preserve the accepted configuration, method, test records, and limitations. If the supplier cannot maintain or explain the earlier state, record that constraint before relying on rollback as a remedy. Historical outputs should remain linked to the configuration and process under which they were produced.

Use a Validation Impact Record

Figure 1 proposes four decisions: identify the change, assess affected claims, generate proportionate evidence, and authorize use. Assign qualified quality and business owners alongside the provider's technical owner. Distinguish unchanged evidence from claims requiring focused retest or broader reassessment.

Testing should include the complete workflow and relevant human-AI interaction. A generic model benchmark cannot establish suitability for a regulated task. Use representative sources, difficult cases, failure handling, and the intended review process, with predefined acceptance criteria appropriate to the activity.

The UK Software Security Code emphasizes lifecycle maintenance and communication.³ It is voluntary software guidance, not a GxP standard. It reinforces the need for an operational supplier-change route; the regulated organization must separately establish its validation and quality obligations.

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, secs. 4.2–4.3, “Human Review Capacity Against Agent Output Volume” and “Routine Approval of Agent Output at Human Review Points,” <https://doi.org/10.2139/ssrn.7164559>; Hatch, *Agentic AI Outsourcing*, Part 2, “The Shift From Managing People to Managing Agents”; Part 6, “The Executive Action Plan.”

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 validation impact record



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

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

Control Urgent Updates and Ongoing Dependencies

EU, UK, Swiss, US, and other life-sciences requirements differ by product, activity, and applicable quality regime. Qualified specialists should document the relevant conclusions. Do not treat a proposed guideline, internal risk acceptance, or supplier assurance as a substitute for required validation or authorization.

Agree notice, access to evidence, implementation options, temporary restrictions, and the route for urgent security changes. The organization may need to compare the risk of delay with the risk of deploying an incompletely assessed update. Preserve the decision and conditions rather than let urgency remove accountability.

After release, verify the actual configuration and monitor relevant quality signals. Reconcile cases affected by the transition and identify whether prior outputs require review. Restoring the old software does not by itself determine the disposition of work already completed under the new version.

Keep Validation Connected to the Live Service

A reasonable objection is that reassessing every update would prevent useful iteration. Use proportionate change categories and reusable evidence. The necessary decision is whether the affected claims remain supported, not whether every small release requires a complete repeat of all earlier work.

Before accepting a material update, require a concise impact conclusion, supporting tests, qualified approval, operating restrictions, and a monitoring plan. Resolve significant gaps or narrow the permitted use. Retain the history so that an inspector or reviewer can understand the basis for reliance.

The executive should approve the changed service only at the scope the evidence supports. Validation remains useful when it follows the operating reality. A supplier release should trigger the right question about continued suitability rather than silently inherit an approval intended for 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 validation-impact record connecting supplier changes to affected regulated-use claims, proportionate evidence, and qualified release decisions. 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

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>.

US Food and Drug Administration and European Medicines Agency. *Guiding Principles of Good AI Practice in Drug Development*. US Food and Drug Administration and European Medicines Agency, January 2026. <https://www.fda.gov/media/189581/download>.

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