

Critical Third Party Oversight and the Bank's Retained Duty

A Board Review of Agentic Service Dependencies

Phil Hatch | Akholi

October 23, 2026

Direct oversight of critical technology suppliers does not establish that a bank's own agentic service is governed or recoverable. Directors should require a dependency review connecting the primary provider to the bank's actual business service.

Keep the Bank's Responsibility in View

The board risk committee should require management to explain its own exposure to underlying technology suppliers before relying on their regulatory designation. Critical-provider oversight addresses a different level of risk from the bank's decision to outsource a particular service. It cannot determine whether the bank has approved appropriate authority or can continue its own operations.

ESMA describes DORA oversight as complementary to financial entities' own responsibilities. The distinction is explicit: direct oversight of a critical ICT provider does not replace the entity's management of ICT risk. A bank should therefore avoid treating designation as an assurance opinion on its own provider's configuration or service chain.¹

The board decision is to approve a dependency review with named owners and tested continuity assumptions. Management should identify the services that support important business outcomes, the providers behind them, and the consequences of disruption or change. The review must reach dependencies that have not been designated critical.

¹ European Securities and Markets Authority, "DORA Oversight," European Securities and Markets Authority, accessed October 23, 2026, opening description of the oversight framework, <https://www.esma.europa.eu/dora-oversight>.

Trace Dependencies to Business Consequences

A provider's agent may depend on a model host, cloud platform, identity service, orchestration layer, registry, data feed, and business-system interface. A list of supplier names is insufficient. Management should explain which action fails when a dependency is unavailable, degraded, changed, or withdrawn.

The study distinguishes third-party dependencies and delivery visibility from the primary outsourcing relationship. Its accounts illustrate why a working service can conceal untested reliance on an underlying platform. They are reported experiences in the sampled engagements, not an estimate of disruption probability for the bank's portfolio.²

Ask for the path from dependency to customer consequence. A model outage might stop new case processing; an identity failure could prevent investigation; an interface change could produce incorrect updates while the agent still reports success. Different consequences require different monitoring, operating limits, and fallback.

Require a Board Dependency Review

Figure 1 proposes a review organized around the business service. Management should identify the dependency, affected action, substitute or fallback, switching conditions, evidence access, and recovery owner. Aggregate exposure matters when multiple providers rely on the same underlying service, even if each individual agreement appears diversified.

ESMA's Q&A on a non-EU outsourced provider states that responsibility for the entrusted function's operational resilience remains with the EU financial entity when the provider uses ICT services. The bank must understand the chain rather than assume that placing the primary provider outside the EU removes its own DORA responsibilities.³

The review should distinguish a credible substitute from a supplier name on a contingency slide. A substitute needs compatible access, data, tools, permissions, staff, and approved operating procedures. Management should state the expected interruption and the evidence supporting that estimate, including limitations in the test.

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, Third-Party Ecosystem, sec. 6.1, "Mapping of Third- and Fourth-Party Dependencies," <https://doi.org/10.2139/ssrn.7164559>; Hatch, *Agentic AI Outsourcing*, Part 2, sec. 5.1, "Agent Actions Visible Only Inside Each Firm's Own Tools."

³ European Securities and Markets Authority, "Application of DORA for Outsourced Critical Services That Are Not ICT," European Securities and Markets Authority, February 12, 2024, ESMA Q&A 2107, <https://www.esma.europa.eu/publications-data/questions-answers/2107>.

Figure 1. Review the dependency through the business service

Board question	Management answer	Evidence required
What fails	Action and customer consequence	Service dependency map
What is shared	Concentration across providers	Underlying supplier reconciliation
What can replace it	Approved fallback and capacity	Switching and recovery test
Who remains accountable	Bank owner and local duty	Applicability and decision record

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.

Apply Local Regimes Without Confusing Their Scope

The UK critical-third-party regime targets risks to financial-system stability and confidence. Firms still need their own third-party risk management. The board should obtain a UK applicability conclusion for the relevant entity and service rather than import DORA terminology or assume designation creates the same obligations in both systems.⁴

Swiss entities should consider FINMA's observations on AI governance and growing third-party dependence within their own supervisory context. Those observations support scrutiny of responsibility and evidence; they do not make an EU designation a Swiss approval. US entities likewise need a separate analysis of their applicable bank duties.⁵

A common dependency inventory can serve the group, provided local owners document their conclusions. The inventory should retain the legal entity, service scope, relevant contract, approved data location, and notification route. Differences should be resolved in operating instructions before they become conflicts during disruption.

⁴ Bank of England, Prudential Regulation Authority, and Financial Conduct Authority, "Operational Resilience: Critical Third Parties to the UK Financial Sector," Bank of England, Prudential Regulation Authority, and Financial Conduct Authority, November 12, 2024, PS16/24, overview of the regime and retained firm responsibilities, <https://www.bankofengland.co.uk/prudential-regulation/publication/2024/november/operational-resilience-critical-third-parties-to-the-uk-financial-sector-policy-statement>.

⁵ Swiss Financial Market Supervisory Authority, *Governance and Risk Management When Using Artificial Intelligence* (Swiss Financial Market Supervisory Authority, December 18, 2024), FINMA Guidance 08/2024, secs. 2.1–2.7, https://www.finma.ch/~media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmittelungen/20241218-finma-aufsichtsmittelung-08-2024.pdf?hash=60E2745D7AC1D7F4E06CE43474539F68&sc_lang=en.

Test Continuity Under Loss of the Dependency

Management should demonstrate a representative loss scenario for each material concentration. The exercise should establish what can continue, what must stop, how cases are preserved, and which manual or alternative route is genuinely available. A tabletop is useful for decision rights but cannot prove technical switching capability.

Diversification should be assessed by failure mechanism, not supplier count. Two prime providers may depend on the same model endpoint, identity platform, or data source. Conversely, changing a prime provider may introduce transition risk without reducing the relevant concentration. The board should ask management to show which disruption becomes less consequential under each proposed mitigation and what new dependencies it creates. That comparison supports a deliberate exposure decision instead of a numerical diversification target.

The board should challenge fallback capacity. If several services fail together, the same expert team may be expected to recover all of them. A plan that works for one isolated outage can fail under a shared dependency incident. Capacity, access, and prioritization should be tested against the scenario the bank is relying on.

Recovery evidence should include the integrity of completed and incomplete work. Restoring platform availability does not establish that missed cases were recovered or duplicate actions avoided. Management should reconcile the backlog and confirm business acceptance before reporting the service restored.

Approve Exposure with Explicit Conditions

The board should receive material concentrations, untested substitutions, dependency changes, and overdue corrective actions. Management should recommend which exposure to retain, constrain, diversify, or exit, supported by service-level evidence. Regulatory oversight is relevant context within that decision, not a reason to remove the dependency from review.

The bank's retained duty requires an explanation of how its own service operates and recovers through the supplier chain. Directors should approve continuation on that evidence and require renewed review when a dependency or authority changes. A designation cannot answer those institution-specific questions.

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. 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 board dependency review that separates systemic supplier oversight from institution-specific continuity and accountability. 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

- Bank of England, Prudential Regulation Authority, and Financial Conduct Authority. “Operational Resilience: Critical Third Parties to the UK Financial Sector.” Bank of England, Prudential Regulation Authority, and Financial Conduct Authority. November 12, 2024. <https://www.bankofengland.co.uk/prudential-regulation/publication/2024/november/operational-resilience-critical-third-parties-to-the-uk-financial-sector-policy-statement>.
- European Securities and Markets Authority. “DORA Oversight.” European Securities and Markets Authority. Accessed October 23, 2026. <https://www.esma.europa.eu/dora-oversight>.
- European Securities and Markets Authority. “Application of DORA for Outsourced Critical Services That Are Not ICT.” European Securities and Markets Authority. February 12, 2024. <https://www.esma.europa.eu/publications-data/questions-answers/2107>.
- 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>.
- Swiss Financial Market Supervisory Authority. *Governance and Risk Management When Using Artificial Intelligence*. Swiss Financial Market Supervisory Authority, December 18, 2024. https://www.finma.ch/~media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmittelungen/20241218-finma-aufsichtsmittelung-08-2024.pdf?hash=60E2745D7AC1D7F4E06CE43474539F68&sc_lang=en.

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