

Common Infrastructure Risk Across Multiple Service Providers

A Portfolio View of Shared Failure

Phil Hatch | Akholi

October 23, 2026

Executives should measure supplier diversification by independent delivery dependencies, not the number of prime contracts. Different providers can fail together when they rely on the same cloud, model, identity service, or operating bottleneck.

Count Failure Domains Rather Than Logos

The board should ask management which outsourced services can become unavailable at the same time. A supplier portfolio can look diversified by contract while concentrating its real delivery on a small number of infrastructure dependencies. Agentic delivery adds models, orchestration, tool gateways, identity services, and shared data products to that assessment.

BIS authors identify common cloud, software, and frontier-AI dependencies as channels through which disruption can spread across firms and jurisdictions.¹ This is a risk mechanism, not a forecast that a particular supplier will fail. The buyer's task is to identify its own common failure domains and the business functions exposed to them.

Start with the most consequential outcomes the organization purchases. Link each to the prime provider, material subcontractors, technology services, required access, and human recovery resources. A dependency is material when its loss prevents the contracted result or the agreed recovery mode, even if its share of the invoice is small.

¹ Juan Carlos Crisanto et al., "When Machines Attack: Frontier AI Cyber Threats and Policy Responses in the Financial Sector," Bank for International Settlements, Financial Stability Institute, September 9, 2026, publication summary on shared dependencies and response capacity, <https://www.bis.org/publications/fsi-paper-28-when-machines-attack-frontier-ai-cyber-threats-and-policy-responses-financial-sector>.

Map the Dependency Behind the Claimed Alternative

The study identifies incomplete mapping of third- and fourth-party dependencies in banking engagements.² Cross-industry buyers should use that finding to question their own maps, not as an estimate of their failure prevalence. The important distinction is between a named supplier list and an explanation of how the service depends on each supplier.

For a hypothetical claims service, two prime providers may use different applications but the same model endpoint and identity service. Moving volume between the primes would not restore service during the shared outage. Management should identify which alternative changes the relevant dependency and what other constraints the switch introduces.

Record dependency purpose, affected services, location, substitutability, switching prerequisites, and evidence date. Where a provider cannot disclose a sensitive architectural detail, agree a protected assurance route that still permits the buyer to assess common exposure. An undisclosed dependency should remain uncertainty in the decision rather than be counted as independent capacity.

Test the Portfolio Under a Shared Outage

Figure 1 proposes a portfolio decision record. For each selected failure domain, show affected outcomes, minimum service, available alternatives, and the executive decision needed. The exercise should include simultaneous demand on shared fallback staff and tools. The same recovery team cannot be counted at full capacity for every service at once.

Test the claimed substitution with representative work. Confirm that data, permissions, licenses, configurations, and process knowledge are available through the alternative route. A contract option to buy capacity is weaker evidence than a demonstrated ability to complete and reconcile the required work within the relevant service window.

The organization should distinguish a technical alternative from an operationally independent one. A second cloud region may reduce one type of outage while preserving dependence on the same identity or control service. A second model may still rely on the same orchestration gateway. State exactly which scenario the alternative addresses.

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,” indicator C196, <https://doi.org/10.2139/ssrn.7164559>.

Figure 1. The common dependency decision record

Shared failure	Business exposure	Executive evidence
Technology service	Affected contracted outcomes	Dependency and scenario map
Alternative route	Work it can sustain	Representative substitution test
Recovery resources	Competing service demand	Joint staffing and access exercise
Residual exposure	Consequence still retained	Funded action or explicit acceptance

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.

Connect Exposure to Governance and Commercial Choices

UK oversight of designated critical providers complements firms' own contingency duties; it does not replace them.³ EU, Swiss, and US operations require separate applicability analysis. A provider's regulated or designated status should not be treated as proof that the buyer has adequate recovery capacity for its own service.

Management can reduce exposure through architectural separation, reserved recovery resources, narrower authority, better portability, or a deliberate service restriction. Each option has cost and performance consequences. The board should compare these choices against the actual common failure rather than demand a second provider as a universal remedy.

Commercial terms should require timely notice of material dependency changes and evidence needed for the buyer's reassessment. A provider replacing an underlying model or consolidating support teams can alter portfolio exposure without changing the prime contract. The buyer needs a route to investigate that change before counting the service as unchanged.

³ Bank of England, "UK Financial Regulators to Begin Overseeing Critical Third Parties Announced by HM Treasury," Bank of England, July 10, 2026, retained firm responsibilities and notes to editors 23–26, <https://www.bankofengland.co.uk/news/2026/july/uk-financial-regulators-to-begin-overseeing-critical-third-parties-announced-by-hmt>.

Approve the Exposure That Remains

Complete independence may be unavailable or uneconomic. The decision is therefore not whether all common dependencies can be removed, but whether management understands the remaining exposure and can sustain an acceptable service under the selected scenarios. Uncertainty should be visible in that approval.

The committee should receive a short view of shared failure domains, affected business outcomes, tested alternatives, resource conflicts, and funded remediation. Track material changes rather than produce a static annual map. Where an assumption fails, change the recovery plan or risk acceptance rather than leave the original diversification claim intact.

Supplier count is a procurement fact. Independent delivery capacity is an operating conclusion that requires evidence. The board should approve the latter, with clear limits on which shared failures the organization can withstand and which consequences it has chosen to retain.

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 portfolio common-failure record that tests supplier diversification against underlying dependencies, simultaneous recovery demand, and demonstrated substitution. 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. “UK Financial Regulators to Begin Overseeing Critical Third Parties Announced by HM Treasury.” Bank of England. July 10, 2026. <https://www.bankofengland.co.uk/news/2026/july/uk-financial-regulators-to-begin-overseeing-critical-third-parties-announced-by-hmt>.
- Crisanto, Juan Carlos, Adrien Currat, and Jeffery Yong. “When Machines Attack: Frontier AI Cyber Threats and Policy Responses in the Financial Sector.” Bank for International Settlements, Financial Stability Institute. September 9, 2026. <https://www.bis.org/publications/fsi-paper-28-when-machines-attack-frontier-ai-cyber-threats-and-policy-responses-financial-sector>.
- 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>.

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