The supplier you cannot exit

Concentration is a continuity question rather than a procurement one: whether the business can still operate when one supplier changes its price, its terms, its model version or its mind.

DESIGNATED

19
PROVIDERS
Named as critical ICT third parties by the European supervisory authorities, November 2025.

13 Jul 2026
UK REGIME
Four providers brought inside the UK critical third parties rules.

Regulators have started naming the suppliers

In November 2025 the three European supervisory authorities designated the first critical information and communications technology third party providers, or CTPPs, under the Digital Operational Resilience Act, known as DORA. Nineteen were named, among them Amazon Web Services, Microsoft Ireland, Google Cloud, IBM, Oracle, SAP, Accenture, Capgemini and Equinix.[1] Designation brings a lead overseer, an annual oversight plan, joint examination teams, oversight fees paid by the provider, and a public record where recommendations are not followed.[2]

The United Kingdom followed. His Majesty's Treasury designated Amazon Web Services, Google Cloud, Microsoft Ireland and Oracle as critical third parties, or CTPs, with the regime taking effect for them on 13 July 2026, and regulators were explicit that this displaces none of a firm's own obligations.[3]

Two of those facts matter to a board outside financial services. The supervisory map now tells any organisation where the systemic concentration sits, free of charge and in public. And the supervision protects the financial system, not the individual customer: nothing in it stops a supplier changing its terms, retiring a product or suffering an outage that takes a business offline for a day.

THE LADDER

4
RUNGS
Expert review, walkthrough, tabletop, simulation. Ask which one the last test reached.

The exit plan nobody has tested

The regulatory language on exit is unusually blunt. Exit plans for services supporting critical or important functions must be comprehensive, documented and sufficiently tested and reviewed periodically.[4] United Kingdom guidance since 2016 has expected exit plans that are understood, documented and fully tested, and has asked firms to consider what they would do if the provider failed.[5] The Financial Stability Board goes further and warns that exit strategies designed to run over long periods may be of little use against short term disruption.[5]

Testing is a ladder rather than a switch. The European Banking Federation's technical work sets out four rungs: expert review, walkthrough, tabletop exercise, and simulation in a monitored environment; it also says openly that full exit testing can tie up considerable resources and may be disproportionate.[6] That candour is useful, because it converts an unanswerable question into an answerable one. The board does not ask whether exit has been proven. It asks which rung the last test reached, for which service, and on what date.

THE DEADLINE

12 Jan 2027
EGRESS
Switching charges, including egress, must be removed entirely under the Data Act.

Switching is getting cheaper, which is not the same as easy

The Data Act has applied since September 2025. Providers may charge only pass-through costs for switching and data egress until 12 January 2027, after which switching charges including egress must go entirely. The rules also set a maximum two month notice period, porting within thirty days extendable to seven months where that is not feasible, and an obligation on infrastructure providers to remove obstacles to achieving functional equivalence elsewhere.[7]

The voluntary schemes that came before tell a board what to watch for. Examining the free egress programmes announced in 2024, the competition

THE MARKET

15%

EUROPEAN

The share held by European providers in their own market, flat since 2022, against 70% for the three largest.

PUBLISHED NOTICE

1 **Six months**
The longest general commitment published by a major model provider, with three months for variants.

2 **Sixty days**
The minimum another provider and a major platform publish for generally available models.

3 **Two weeks**
What a preview model may get. None of these are contractual terms.

ONE EVENT

14h 32m

OCTOBER 2025

A single region's failure at the largest provider, from one latent fault in a name management system.

authority found minimum data volumes, sixty day windows, pre-approval requirements, exclusion of partial switching and of continuing multi-cloud use, a requirement to close the account, and terms the providers could change at will; it concluded that sixty days was unlikely to be enough where a switch takes months or years.[8] Egress was never the expensive part. Re-architecture is, and no regulation removes it.

Three providers hold seventy per cent

European providers held fifteen per cent of their own regional market in the first half of 2025, flat since 2022 and down from twenty-nine per cent in 2017, while the three largest United States providers held seventy per cent.[9] The United Kingdom competition authority's market investigation concluded in July 2025 with three adverse findings: concentration and barriers to entry, technical and commercial barriers to switching, and licensing practices that reduce competition in cloud markets.[10]

What happened next is instructive about the pace of remedy. In March 2026 the authority declined to open strategic market status investigations into cloud, accepting voluntary commitments on egress fees and interoperability instead, and turned its statutory attention to business software licensing.[10] In June 2026 the European Commission reached the preliminary position that the two largest cloud services in the Union should be designated under the digital markets regulation.[11] A board should assume that structural remedy arrives slowly, and that in the meantime the negotiating position is its own to build.

The AI dependency is shorter dated than the cloud one

Cloud migrations are measured in years. Model lifecycles are measured in months, and the published commitments are modest. One major provider undertakes at least six months' notice for generally available models, three months for specialised variants, and as little as two weeks for previews. Another commits to at least sixty days. A major platform sets retirement programmatically at eighteen months from a model's launch, not from a customer's adoption, with a minimum of sixty days' notice, no automatic upgrade for provisioned deployments, and requests failing outright after retirement. Another marks models legacy for six months, or forty-five days in some cases, and can withdraw access after a fortnight of inactivity.[12]

These are published lifecycle policies rather than contractual rights. Version pinning exists as a dated model snapshot, which is a technical convenience the provider can retire, not a commitment it has made to the customer. That distinction is the one sentence on this subject a board needs to hold: the roadmap is the supplier's, and the dependency is the organisation's.

The effect is not theoretical. Through 2026 consumer and enterprise users of one assistant were moved off several model versions on published dates, including versions withdrawn from custom deployments for business and education customers.[12] Anything built tightly around a specific model's behaviour inherits that calendar.

When it fails, it fails wide

October 2025 produced two demonstrations within a fortnight. A regional failure at the largest provider ran for about fourteen and a half hours, caused by a latent race condition in the domain name management of a database service, and took out a long list of dependent services.[13] Ten days later a configuration change pushed globally to a content delivery control plane disrupted portals, identity, databases and office services; geographic redundancy gave no protection, because every node received the same change.[13] In November a content delivery provider's failure of under six hours took a major AI assistant offline with it.[13]

In May 2026 simultaneous cooling failures in a single data hall triggered thermal shutdowns; one exchange halted trading for around eight hours and took a further twelve to reach full recovery.[13] The Financial Policy Committee has since warned in plain terms that a compromise or defensive shutdown at a common supplier could affect several institutions at once, and named reliance on a handful of frontier AI providers as part of that picture.[14] Resilience is now a question about correlation, not about uptime percentages.

OUTSIDE FINANCE

24h

NOTIFICATION

The initial reporting window proposed in the UK cyber security and resilience bill, with a fuller report at 72 hours.

The obligations are arriving outside financial services

Supply chain security is already a legal obligation for a wide range of organisations under the network and information security directive, which requires measures addressing the relationship with direct suppliers and an assessment of each supplier's own practices.[15] Transposition has been uneven: the Commission referred four member states to the Court of Justice in July 2026 for failing to notify full transposition.[15] A group operating across several member states faces one obligation expressed at several different speeds.

In the United Kingdom the cyber security and resilience bill, introduced in November 2025 and still before Parliament, would bring medium and large managed service providers and data centres into scope, allow regulators to designate critical suppliers, and require notification of significant incidents within twenty four hours and a fuller report within seventy two.[16] United Kingdom data centres, including those used by the largest cloud operators, were designated critical national infrastructure in September 2024.[16] The direction is consistent: the supplier relationship is becoming a regulated object in its own right, and the board that already knows its dependencies will find the reporting straightforward.

THE CONVERSION

1

QUOTATION

A priced alternative held on file is what turns a dependency into a negotiation.

Ninety days of useful work

1. Name the three suppliers whose failure would stop the business, and say for each how long the business could run without them. Not an estimate: a tested figure, with a date.
2. Ask which rung of the testing ladder the last exit test reached, and book the next one at the rung above.
3. Get the model lifecycle terms out of the documentation and into the contract: notice period, version availability, and what happens to a pinned version.
4. Check that the architecture can name a model version in configuration rather than in code, so that a forced migration is a change request, not a project.
5. Price the second supplier before it is needed. A quotation held on file is what converts a dependency into a negotiation.
6. Put the correlated failure question to the executive: which of our critical services would fail together, and which share one provider, one region or one control plane?
7. Fold supplier concentration into the risk register as a named risk with an owner, rather than leaving it inside a procurement paper nobody reads twice.

Some dependencies are chosen, others inherited

Nobody proposes leaving the large providers, and few organisations should. The decision worth making is narrower and more useful: knowing which dependencies are deliberate, which were inherited, and what each would cost to unwind if the terms changed. Substitutability is a commercial property rather than a technical one, and it decays quietly unless someone is asked to prove otherwise. The discipline is small: name the dependency, price the alternative, test the exit one rung deeper than last time.

Twelve questions, and the answers that should worry you

Ask the executive	Worry if the answer is
Which three suppliers could stop this business, and for how long?	“We are resilient.” Ask for three names and three durations.
When did we last test an exit, and at what depth?	“We have an exit plan.” A document is a rung below a walkthrough.
What would it cost to move our largest workload?	“Egress is free now.” Egress was never the expensive part.
What notice do we get before a model version we rely on is retired?	“The vendor gives plenty of notice.” In the contract, or in the documentation?
Is the model version named in configuration, or written through the code?	“The developers handle that.” It decides whether migration is a change or a project.
Which critical services share a provider, region or control plane?	“We are multi-region.” One control plane defeats many regions.
Who is our second supplier, and when did we last price it?	“We could go elsewhere if needed.” Ask for the quotation and its date.
What did the October 2025 and May 2026 outages cost us?	“We were not materially affected.” Ask who measured it, and how.
Are we inside any regulator's critical third party perimeter?	“That only applies to banks.” It tells everyone where the concentration sits.
What happens if this supplier raises prices by a fifth at renewal?	“We would negotiate.” With what alternative, priced when?
Who owns concentration as a risk, and where is it reported?	“It sits with procurement.” Procurement buys; it does not carry continuity.
Which of these answers came from evidence rather than assumption?	A pause. That pause is the finding.

NOTES AND SOURCES

1 European Supervisory Authorities, designation of critical ICT third party providers, 18 November 2025; the list of nineteen as reported by PwC Legal the same day.

2 ESAs, *Guide on DORA oversight activities* JC 2025 29, 15 July 2025.

3 Bank of England and HM Treasury, first critical third party designations, announced 10 July 2026, in effect 13 July 2026.

4 Regulation (EU) 2022/2554 (DORA), Article 28(8); in application since 17 January 2025.

5 Financial Conduct Authority, FG16/5, July 2016, updated September 2019; Financial Stability Board, *Enhancing third-party risk management and oversight*, Tool 3.7, 4 December 2023.

6 European Banking Federation Cloud Banking Forum, *Cloud exit strategy: testing of exit plans*, 4 June 2020.

7 Regulation (EU) 2023/2854 (Data Act), Articles 23 to 26; applicable since 12 September 2025.

8 Competition and Markets Authority, cloud services market investigation, Appendix N, 28 January 2025.

9 Synergy Research Group, European cloud provider share, 24 July 2025.

10 Competition and Markets Authority, cloud services market investigation, summary of final decision, 31 July 2025, and package of actions on business software and cloud services, 31 March 2026.

11 European Commission, preliminary position on cloud gatekeeper designation under the Digital Markets Act, 25 June 2026.

12 Published model deprecation and lifecycle policies of OpenAI, Anthropic, Microsoft Foundry and Amazon Bedrock, and OpenAI's ChatGPT model retirements of February to April 2026, as at 17 September 2026.

13 AWS post-event summary, us-east-1, 19 to 20 October 2025; ThousandEyes on Azure Front Door, 29 to 30 October 2025; Cloudflare, 18 November 2025; IT Pro, 8 May 2026, and the Coinbase post-mortem, 1 June 2026.

14 Bank of England, *Financial Stability Report*, 7 July 2026.

15 Directive (EU) 2022/2555 (NIS2), Article 21(2)(d) and 21(3); European Commission referral of four member states to the Court of Justice, 8 July 2026.

16 Cyber Security and Resilience (Network and Information Systems) Bill, introduced 12 November 2025, before the House of Lords as at September 2026; UK data centres designated critical national infrastructure, 12 September 2024.

AltLibre Papers, board series, paper 03 of five. Adrian Hollister, AltLibre, 5 September 2026. altlibre.com