INFRASTRUCTUREOUTSIDETHEPERIMETER · PART2OF4

The Provider You Cannot Exit

Cloud Concentration and the Regulated Firm

David Newns, Substrate Advisory
July 2026

1. The structural fact

In the first quarter of 2026, enterprise spending on cloud infrastructure services reached 129 billion US dollars, an annual run rate above half a trillion dollars, growing at 35 per cent year on year. Three US-headquartered providers took 63 per cent of it: Amazon Web Services at 28 per cent, Microsoft at 21 per cent and Google at 14 per cent. No other provider approaches their scale, and no European provider features among the leaders: the largest, SAP and Deutsche Telekom, hold 2 per cent each of the European market.[1]

The thesis of this series is that each of four technologies, AI, cloud, public blockchain infrastructure and post-quantum cryptography, is driving changes in the regulatory environment, and that a licensed firm has three postures available: respond, exploit or ignore. For cloud, the regulatory change is the most concrete of the four. Within nine months, both the EU and the UK moved the providers themselves inside the supervisory perimeter: the European Supervisory Authorities designated nineteen Critical ICT Third-Party Providers under DORA on 18th November 2025,[2] and HM Treasury designated the first four UK Critical Third Parties with effect from 13th July 2026.[3] The question a board faced five years ago was whether it was permitted to outsource to the cloud. The question it faces now is whether it can evidence, to a supervisor with direct oversight of its provider, that it understands the dependency in detail and could survive its loss. The October 2025 US-EAST-1 outage demonstrated what that dependency looks like when it fails,[4,5] and 2026 is the first year in which the firm-side evidence, exit strategies and registers of information, is being tested at scale.

2. The dependency as it stands

The headline market shares understate the concentration, because the dependency operates at three levels beneath the provider name on the contract.

The first level is the provider itself. Exit from one of the three to another is feasible, at cost and over time, and EU law now requires firms to plan for it. Exit from the group of three is theoretical: there is no European hyperscaler and no domestic substitute at the relevant scale. The fastest-growing challengers, the AI-focused neoclouds, held around 5 per cent of the market in the first quarter of 2026 and sell GPU capacity rather than the full managed-service estate a bank runs on.[1]

The second level is the service. Cloud services sit on a portability gradient. Raw compute, storage and networking are close to commoditised and move between providers with engineering effort that is estimable in advance. Proprietary managed services, the databases, queues, identity systems and serverless platforms that make cloud economically attractive, have no functional equivalent elsewhere: a workload built on one provider's managed database is rebuilt, not migrated. The commercial logic of the hyperscaler model pushes customers up this gradient, because the managed services carry the margin and the lock-in together. A firm's true substitutability is set by the least portable service on its critical path, and that is rarely visible in a contract-level inventory.

The third level is the region, and it is the least understood at board level. On 20th October 2025, the AWS US-EAST-1 region failed because of a latent race condition in the automated DNS management of its DynamoDB service, and the cascade disrupted services worldwide for roughly fifteen hours.[4] The reported UK impact included HM Revenue and Customs and the Lloyds Banking Group brands, and the outage drew questions from the chair of the Commons Treasury Committee to HM Treasury on why UK banking and tax infrastructure had been interrupted from a US region and on whether the provider should be designated a Critical Third Party.[5] The supervisory significance is architectural: firms whose workloads ran entirely inside

European regions were affected, because certain global services, identity and access management among them, are homed in US-EAST-1, and workloads that depend on them inherit that single-region dependency.[4,5] A firm can buy European data residency and still carry a North Virginia control-plane dependency it has never inventoried.

What the firm and its supervisor can reach maps onto these levels unevenly. The contract is reachable and always has been. The provider's resilience is now partially reachable, through the oversight regimes described below. The parent company's legal position is not reachable by either: the US CLOUD Act, enacted in 2018, allows US authorities to compel US-headquartered companies to produce data they control, wherever that data is physically held.[6] On 10th June 2025, the Director of Public and Legal Affairs at Microsoft France was asked under oath by a French Senate commission of inquiry whether he could guarantee that French citizens' data held by Microsoft would not be passed to US authorities without French authorisation, and answered "non, je ne peux pas le garantir", adding that it had never yet happened.[7] That is the position of the second-largest cloud provider in Europe, on the record before a parliamentary committee. Justified and arbitrary exercises of that legal reach produce identical operational consequences for the firm whose data or service is affected, which is why the exposure belongs in an operational risk register rather than a political analysis.

3. The regulatory response in motion

European Union. DORA has applied to financial entities since 17th January 2025. Two of its mechanisms matter most here. Article 28 obliges firms to maintain a register of information covering all ICT third-party contractual arrangements and to hold documented exit strategies for services supporting critical or important functions.[8] The register is the instrument through which the whole oversight edifice sees: national authorities collect the registers annually, forward them to the ESAs, and the ESAs use the aggregated data to designate critical providers. The first designations followed on 18th November 2025, when the ESAs named nineteen Critical ICT Third-Party Providers, the three hyperscalers among them alongside Oracle, IBM, SAP and Deutsche Telekom.[2] Each CTPP now has a Lead Overseer drawn from one of the three ESAs, supported by Joint Examination Teams of ESA and national-authority staff, with powers to request information, conduct investigations and inspections, issue recommendations and impose periodic penalty payments.[9] The first complete oversight cycle, including initial examinations, runs through 2026.[10]

The register obligation is proving harder than it looks. In the ESAs' 2024 dry run, close to a thousand financial entities submitted registers on a best-effort basis, and 6.5 per cent passed all data quality checks, a result the ESAs judged in line with expectations for a voluntary exercise while calling for further industry effort before the live cycle.[11] The 2026 cycle, reporting the position as at 31st December 2025, is mandatory, with national deadlines that ran through March 2026 and ESA-level quality checks following. A firm whose register cannot survive validation is telling its supervisor, in machine-readable form, that it does not know its own dependency.

Alongside DORA sits the EU Data Act, which has applied since 12th September 2025 and attacks the commercial side of lock-in.[12] Its switching provisions require cloud contracts to specify maximum notice periods and support for migration, require functional equivalence for infrastructure services and phase out switching charges: until 12th January 2027 providers may charge only their direct costs, and from that date switching charges, including data egress fees for the switching process, are prohibited outright.[13] Chapter VII separately requires providers operating in the EU to take technical, legal and organisational measures against unlawful third-country governmental access to data held in the Union,[12] which is the EU legislature's answer to the exposure Microsoft France described under oath; whether contractual and organisational

measures can override the compelled position of a US parent remains untested. The European Central Bank published its guide on outsourcing to cloud service providers in July 2025,[14] and the European Commission's Cloud Sovereignty Framework of October 2025 gives public procurement a scored methodology for assessing sovereignty claims,[15] a document worth reading even for private-sector buyers because it decomposes sovereignty into assessable criteria rather than a label.

United Kingdom. The critical third parties regime made under the Financial Services and Markets Act 2023 took effect on 1st January 2025,[16] and sat without designations for eighteen months. On 10th July 2026, HM Treasury designated the first four: AWS EMEA SARL, Google Cloud EMEA Limited, Microsoft Ireland Operations Limited and Oracle Corporation UK Limited, with the Bank of England, PRA and FCA beginning joint oversight on 13th July 2026.[3,17] Oversight is limited to the resilience of the systemic services provided to the UK financial sector, designation is explicitly not authorisation, and the programme is rolling, with further designations possible where the statutory criteria are met.[3,17] The UK list is notable for what it shares with the EU list: the same three hyperscalers plus Oracle appear in both, which means the concentration the regimes were built to oversee is itself concentrated.

Switzerland. FINMA's Circular 2023/1 on operational risks and resilience took effect on 1st January 2024, requiring banks to identify critical functions, set tolerances for disruption and map the supporting resources including third parties, with the 2018/3 outsourcing circular continuing to apply.[18] FINMA reported that as at 2024 one in five Swiss banks or insurers was already outsourcing significant data or functions to public cloud providers.[19]

Sanctions reach. One supervisory document takes the compelled-termination exposure seriously: the Liechtenstein FMA's Communication 2024/2 on the risk management of foreign sanctions law, which addresses the consequences of US sanctions reach for firms in a non-US financial centre and expects it to be managed as a risk rather than assumed away.[20]

International. The FSB's December 2023 toolkit for third-party risk management remains the reference for the cross-jurisdictional picture, with its emphasis on critical services, systemic third-party dependencies and the limits of firm-by-firm supervision of a shared dependency.[21]

The direction across all of these instruments is consistent: from permission to outsource, through firm-level risk management, to direct oversight of the providers, with the commercial barriers to switching being legislated away in parallel. What no instrument yet answers is the systemic question of what the financial sector does if one of the three providers loses operational continuity for several days. Both the EU and UK regimes are oversight of providers, not contingency for their loss.

4. What response looks like

The compliance floor is set by DORA and its UK and Swiss counterparts. The work that distinguishes a well-run firm sits above it, in four areas.

Inventory at the right granularity. The register of information compels a contract-level inventory. The dependency operates at service and region level, so the internal inventory should go one level deeper than the regulatory submission: for each critical or important function, the named services it consumes, the regions those services run in and the global control-plane services they depend on. The US-EAST-1 event is the test case: a firm whose inventory could not have predicted its own exposure to a North Virginia regional failure had an inventory of the wrong resolution.[4] In my experience operating a licensed financial market infrastructure, this mapping is laborious the first time and close to mechanical thereafter, and it changes the

quality of every conversation with the provider, the supervisor and the board.

Exit plans that have met reality. DORA requires exit strategies for critical and important functions.[8] A strategy document is the floor. The distinguishing questions are whether the exit has ever been exercised in test, what it cost, how long it took and what broke. For portable workloads, a test migration of a representative service establishes the real timeline. For workloads on proprietary managed services, the honest output of the exercise is usually the admission that exit means rebuild, at which point the board's choice is to accept that dependency deliberately, with documented compensating controls, or to re-architect the critical path onto portable components. Both are defensible positions. Holding an exit plan that assumes portability the architecture does not possess is not. The Data Act improves the economics of all of this from 12th January 2027, when charging for the switching process ends,[13] and contract renewals crossing that date are the natural point to reset terms.

Contractual reach. The DORA-class contractual provisions, audit and access rights, termination assistance, sub-outsourcing transparency, are compelled. Beyond them, the terms worth negotiating are notification of governmental demands to the extent the provider is lawfully able, data localisation options with the control-plane position stated explicitly rather than implied and transition assistance priced and scoped before it is needed rather than negotiated during an exit.

Sovereign offerings assessed structurally. The sovereign-cloud market is answering a real demand, and the offerings differ in what they actually change. Sovereignty decomposes into at least three dimensions: where the data resides, who operates the infrastructure day to day and who ultimately controls the operating company. AWS launched its European Sovereign Cloud to general availability on 15th January 2026, a physically and logically separate partition in Brandenburg with its own control plane, EU-resident staffing and a dedicated European governance structure of German-incorporated operating companies and an advisory board.[22] That moves the first two dimensions. The third is unchanged: the ultimate parent remains a US-headquartered group, and the legal analysis under the CLOUD Act follows corporate control, not data location or the nationality of the operating entities.[6] A different structural answer is the arrangement the Luxembourg supervisor CSSF adopted in December 2024, in which a locally owned joint venture operates an air-gapped instance of licensed US technology,[23] moving the operator dimension to a local entity while retaining the technology dependency. Neither answer is wrong. A buyer should simply be able to say which dimension it is paying for, because the premium is material and the term sovereign does not distinguish them.

The board-level metrics that fall out of this work are short: the share of critical functions by provider and by region, the count of critical functions on services with no functional equivalent, the tested rather than asserted time-to-exit and the status of the day-three contingency. That contingency is the plan for a provider-level outage lasting days rather than hours: which critical functions continue in degraded mode, what pre-agreed alternative capacity or manual fallback carries them and how clients and the supervisor are kept informed while it does. The skills implication is one senior engineer-economist who understands cloud pricing, egress and portability at the architecture level, a capability most firms below the top tier do not hold and can hire or retain fractionally.

5. The advantage case

The advantage available here is positional rather than dramatic, and should be stated at its actual weight.

The first advantage is supervisory. The register data now flows to national authorities and the ESAs annually, and the 2024 dry run established how rare a clean submission is.[11] A firm whose register

validates, reconciles to its architecture and supports a credible exit narrative is distinguishable to its supervisor in a way that was not previously measurable, and that distinction carries into authorisation processes, thematic reviews and the tone of ongoing supervision.

The second is commercial. Counterparty due diligence increasingly asks the same questions supervisors do, and institutional clients with their own DORA obligations must evidence their sub-outsourcing chain, which makes a firm with a clean dependency story an easier vendor to approve. The end of switching charges in January 2027 shifts negotiating leverage at renewal toward buyers who have done the portability work, because the credible threat of moving is what the fee removal makes cheaper.[13]

The third is access to sovereignty-sensitive demand: public-sector mandates scored under the Commission's framework,[15] and private clients whose confidentiality expectations make the structural analysis above a selling point.

Where the case is thin, it should be said to be thin. There is little published evidence that multi-cloud architectures deliver price advantages; the premium of running dual-provider capability is real and the return is resilience and optionality, not cost. Firms should buy it as insurance, priced against the outage record, rather than expect it to pay for itself.

6. The cost of ignoring it

The documented record is sufficient without embellishment. The October 2025 outage removed a single region for roughly fifteen hours and interrupted, among much else, a G7 tax authority and one of the largest UK retail banking groups, reaching firms whose workloads ran entirely inside European regions.[4,5] The questions put to HM Treasury by the chair of the Commons Treasury Committee asked why national infrastructure had been interrupted from a US region and whether the provider should be brought inside the perimeter,[5] and within nine months it was, in both the EU's designations of November 2025 and the UK's of July 2026.[2,3] A firm that cannot answer those same questions about its own estate is behind its own legislature.

On the compliance floor, the 2024 dry run's 6.5 per cent pass rate is the published baseline for what supervisors received when submission was voluntary.[11] The 2026 cycle is mandatory, feeds the designation and oversight machinery directly, and gives national authorities an objective, comparable measure of each firm's grip on its own dependency. As at July 2026 there is no published European enforcement action specifically for cloud exit-plan failure at a financial institution; the machinery that would produce one, oversight findings flowing from Joint Examination Teams and register data flowing from firms, became operational this year. The firms that appear in the first such actions will be the ones whose registers did not validate and whose exit plans had never been tested, and both of those facts are already visible to their supervisors.

7. Board questions

1. For each critical function, can the executive name the provider, the region and the global control-plane services beneath it, and does our register of information reconcile to that map?
2. When was our exit plan last executed in test, for which workload, at what cost and over what timeline?
3. Which critical functions run on proprietary managed services with no functional equivalent, and can we show that each such dependency was accepted deliberately with compensating controls, rather than accumulated?

4. What is our plan for day three of a provider-level outage, as distinct from a zone or region failure, and has it been exercised?
5. What is our exposure to compelled termination or interruption of service under foreign legal process, and what do our contracts provide on notification and transition assistance?
6. Where we are buying or considering a sovereign cloud offering, which of data residency, operational autonomy and corporate control does it actually change, and is that the dimension we need?
7. Which of our contracts renew after 12th January 2027, and what will we renegotiate when switching charges end?

8. Sources and notes

1. Synergy Research Group, Q1 2026 cloud infrastructure market data (quarterly revenues 129 billion US dollars, growth 35 per cent year on year, worldwide shares AWS 28 per cent, Microsoft 21 per cent, Google 14 per cent; neoclouds approximately 5 per cent of the market), 29th April 2026: https://www.srgresearch.com/articles/cloud-market-annual-revenue-run-rate-topped-half-a-trillion-dollars-in-q1-as-growth-surge-continues See also Synergy Research Group, "European Cloud Providers' Local Market Share Now Holds Steady at 15%", April 2026 (Amazon, Microsoft and Google at 70 per cent of the European market; SAP and Deutsche Telekom the largest European providers at 2 per cent each, followed by OVHcloud, Telecom Italia, Orange and others): https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15
2. Joint ESAs communication, designation of nineteen Critical ICT Third-Party Providers under DORA Article 31, 18th November 2025: https://www.eba.europa.eu/publications-and-media/press-releases/european-supervisory-authorities-designate-critical-ict-third-party-providers-under-digital
3. HM Treasury, "UK financial system strengthened with new safeguards for major technology providers," 10th July 2026 (designation of Amazon Web Services EMEA SARL, Google Cloud EMEA Limited, Microsoft Ireland Operations Limited and Oracle Corporation UK Limited as Critical Third Parties with effect from 13th July 2026): https://www.gov.uk/government/news/uk-financial-system-strengthened-with-new-safeguards-for-major-technology-providers
4. AWS post-event summary, US-EAST-1 service disruption, 20th October 2025 (latent race condition in DynamoDB automated DNS management): https://aws.amazon.com/message/101925/
5. Computer Weekly, "Government faces questions about why US AWS outage disrupted UK tax office and banking firms," October 2025 (UK impact including HMRC and Lloyds Banking Group; questions from the chair of the Commons Treasury Committee to HM Treasury including on Critical Third Party designation of the provider): https://www.computerweekly.com/news/366633473/Government-faces-questions-about-why-US-AWS-outage-disrupted-UK-tax-office-and-banking-firms
6. US CLOUD Act (Clarifying Lawful Overseas Use of Data Act), enacted 23rd March 2018: https://www.congress.gov/bill/115th-congress/house-bill/4943
7. Anton Carniaux (Microsoft France), French Senate commission of inquiry hearing, 10th June 2025. French Senate, compte rendu of the hearing: https://www.senat.fr/compte-rendu-commissions/20250609/ce_commande_publique.html Note: the question, put by the rapporteur, concerned the data of French citizens entrusted to Microsoft through the UGAP public procurement channel; the answer continued that such a transfer had never yet occurred.
8. Regulation (EU) 2022/2554 (Digital Operational Resilience Act), applying from 17th January 2025; Article 28 on the register of information and exit strategies, Article 30 on contractual provisions: https://eur-lex.europa.eu/eli/reg/2022/2554/oj
9. ESAs, "Guide on DORA oversight activities," JC 2025 29, July 2025 (Lead Overseer model, Joint Examination Teams, oversight powers): https://www.esma.europa.eu/sites/default/files/2025-07/JC_2025_29__DORA_Guide_on_oversight_activities.pdf
10. Joint Committee of the European Supervisory Authorities, 2026 Work Programme (first complete oversight cycle, individual annual oversight plans, initial examination activities in 2026): https://www.esma.europa.eu/sites/default/files/2025-10/JC_2025_33_Joint_Committee_of_the_European_Supervisory_Authotities_2026_Work_programme.pdf
11. ESAs, summary report of the 2024 Dry Run exercise on reporting the registers of information under DORA, 17th December 2024 (registers from close to 1,000 financial entities; 6.5 per cent passed all data quality checks): https://www.eiopa.europa.eu/esas-dry-run-exercise-shows-goal-reporting-registers-information-under-digital-operational-2024-12-17_en

12. EU Data Act, Regulation (EU) 2023/2854, applying from 12th September 2025; Chapter VI on switching between data processing services, Chapter VII on international governmental access: https://eur-lex.europa.eu/eli/reg/2023/2854/oj
13. European Commission, "Data Act explained" (gradual withdrawal of switching charges; prohibition of switching charges including data egress from 12th January 2027): https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained
14. ECB Guide on outsourcing cloud services to cloud service providers, 16th July 2025: https://www.bankingsupervision.europa.eu/press/pr/date/2025/html/ssm.pr250716~c0401b1b6b.en.html
15. European Commission, Cloud Sovereignty Framework (criteria, SEAL assurance levels and scoring methodology for cloud-service sovereignty), 20th October 2025: https://commission.europa.eu/document/09579818-64a6-4dd5-9577-446ab6219113_en
16. FCA, PRA and Bank of England, PS24/16 "Operational resilience: Critical third parties to the UK financial sector," 12th November 2024; final rules effective 1st January 2025: https://www.fca.org.uk/publications/policy-statements/ps24-16-operational-resilience-critical-third-parties-uk-financial-sector
17. Bank of England, "UK financial regulators to begin overseeing Critical Third Parties announced by HMT," July 2026 (oversight from 13th July 2026; designation under the regime is not the same as authorisation): https://www.bankofengland.co.uk/news/2026/july/uk-financial-regulators-to-begin-overseeing-critical-third-parties-announced-by-hmt
18. FINMA Circular 2023/1, "Operational risks and resilience - banks," in force 1st January 2024: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023-01-20221207.pdf
19. FINMA, "Cyber risks and outsourcing (2024)" (as at 2024, one in five Swiss banks or insurance companies outsourcing significant data or functions to public cloud service providers): https://www.finma.ch/en/documentation/dossier/dossier-cyberrisiken/cyberrisiken-und-outsourcing-2024/
20. FMA Liechtenstein, Communication 2024/2, "Risk management regarding foreign sanctions law," September 2024: https://www.fma-li.li/fma-li/documents/rechtsgrundlagen/en/fma-communication-2024_2---risk-management-regarding-foreign-sanctions-law.pdf
21. Financial Stability Board, "Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities," 4th December 2023: https://www.fsb.org/2023/12/fsb-publishes-toolkit-for-enhancing-third-party-risk-management-and-oversight/
22. Amazon, "AWS Launches AWS European Sovereign Cloud and Announces Expansion Across Europe," 15th January 2026 (general availability of the Brandenburg region; physically and logically separate infrastructure; EU-based operation; dedicated European governance structure with German-incorporated operating companies and an advisory board): https://press.aboutamazon.com/aws/2026/1/aws-launches-aws-european-sovereign-cloud-and-announces-expansion-across-europe
23. CSSF, "The CSSF adopts Clarence to develop artificial intelligence with full sovereignty," December 2024 (LuxConnect and Proximus Luxembourg joint venture operating an air-gapped instance of Google Distributed Cloud Hosted): https://www.cssf.lu/en/2024/12/the-cssf-adopts-clarence-to-develop-artificial-intelligence-with-full-sovereignty-a-major-breakthrough-for-the-financial-sector/

David Newns is an Advisor to BPX Markets Limited and an Independent Non-Executive Director of Axiology Group. The views expressed are personal and do not represent the positions of any organisation with which he is associated. Nothing in this report constitutes legal, regulatory or investment advice.