ECIPE | EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY

ECIPE Policy Brief – No. 03/2026

Cloud Resilience and Security: Why Exit, Portability, and Lifecycle Design Matter

By **Matthias Bauer** *and* **Dyuti Pandya**, *Director and Analyst at ECIPE.*

EXECUTIVE SUMMARY

The future of computing points to cloud services remaining deeply embedded across sectors. As cloud technologies converge with edge networks and connected devices, resilience and security are no longer secondary technical issues but central policy concerns.

This paper shows that resilience is strengthened not by isolation or localisation mandates, but by preserving architectural choice, interoperability, and competitive multi-cloud options across the lifecycle. Many of the decisive factors that affect resilience occur at onboarding – how a cloud provider, tools, licences, and security controls are selected and integrated – and whether workloads and safeguards can in practice be reconfigured, substituted, or exited during disruption.

Across business, standards, cybersecurity, and competition communities, resilience is understood as a structural property of architecture, governance, and contractual control. The key test is whether organisations retain credible choices at every stage of the cloud journey, from migration to multi-cloud to exit. Concentration becomes a risk only when portability and switching are restricted in practice.

Following a Request for Proposals, the study was commissioned by the Open Cloud Coalition to review barriers to cloud customer choice and greater interoperability in the EU cloud market.

The analysis shows that ending restrictive licensing and contractual practices are the most effective policy lever for strengthening resilience. Licensing determines what can be deployed at onboarding and whether workloads can be duplicated, migrated, or recovered under stress. Restrictions on licence mobility, discriminatory pricing, licensing practices that require re-purchase upon migration or dual-running, and limits on redundancy transform scale into dependency on a single cloud vendor.

By contrast, prescriptive technical regulation to try and address cloud reliability carries higher risk. Cloud architectures and security ecosystems are complex and evolve rapidly, and even specialist engineers rarely have full visibility across dependency chains.

Software equivalence should become a functional requirement, ensuring comparable performance, security, and service levels across cloud environments, rather than a requirement to use the same architecture or interfaces. In practice, this means that cloud and software vendors should not offer degraded functionality, security updates, or support conditions when their products run on third-party clouds compared to their own infrastructure. Mandating technical designs or standardised interfaces, by contrast, risks reducing architectural diversity and increasing correlated failure risks. Resilience is therefore best supported through proportionate, technology-neutral policy focused on preserving lifecycle multi-cloud choice rather than redesigning infrastructure.

Competition also has a constructive role when it targets practices that restrict lifecycle choice rather than focusing narrowly on market shares. Enforcement against discriminatory licensing, tying practices, and artificial switching barriers aligns competition objectives with operational resilience and critical infrastructure protection. The Digital Markets Act (DMA) could contribute positively where it removes contractual barriers to switching and choice and interoperability. By contrast, applying platform-style technical obligations indiscriminately to cloud services risks weakening specialised environments, narrowing security tool choice, and reducing practical exit options.

Policy Implications

Effective resilience policy should:

- prioritise portable and non-discriminatory licensing practices, including the ability to transfer existing software entitlements across cloud environments;
- preserve the ability to onboard independent applications and security tools, including parity in product functionality across clouds;
- avoid prescriptive technical mandates that narrow architectural diversity and increase correlated failure risk;
- focus competition enforcement on contestability and practical exit across the service lifecycle rather than concentration or market shares alone;
- address contractual and licensing practices that raise rivals' costs or restrict customers' ability to deploy workloads on the cloud of their choice, in line with recent CMA findings on partial foreclosure risks; and
- pursue "digital autonomy" in an open manner that sustains access to global standards, interoperable technologies, and international innovation ecosystems.

Cloud resilience and security are ultimately delivered not by managing market structure or redesigning complex technologies through regulation, but by protecting lifecycle choice – especially the practical ability to adapt, migrate, and recover when conditions change.

1. INTRODUCTION: CLOUD CONSOLIDATION, RESILIENCE AND SECURITY

Modern economies now rely heavily on continuous computing and data processing to support public services, business activities, and critical infrastructure. Cloud computing, together with big data analytics and the Internet of Things (IoT), underpins remote processing, service delivery, and real-time operations across the economy. As critical systems increasingly migrate from local environments to the cloud, the resilience of cloud infrastructure increasingly determines the risk of service disruption and data loss, with broad societal and economic implications. Recent large-scale cloud outages make this dependence visible. Even short-lived but widespread technical failures can disrupt services across multiple platforms and temporarily restrict access to data, revealing critical infrastructure chokepoints.[1] As organisations integrate more third-party tools, AI-enabled services, and sector-specific applications into cloud environments, this reliance continues to deepen, particularly in highly regulated sectors pursuing digital modernisation and enhanced cybersecurity.

1.1 Concentration, Dependency and Structural Lock-in

Recognising these risks, regulatory agencies have begun to intervene. For example, European financial market regulators (EBA, EIOPA, and ESMA) have designated 19 technology providers as critical third-party ICT service providers for the financial sector.[2] Under the Digital Operational Resilience Act (DORA), which entered into force in January 2025, EU-level regulators (under Article 31 (9) DORA) are empowered to identify and directly oversee such providers with the aim of mitigating systemic vulnerabilities associated with dependencies on external infrastructure.

While many of the designated providers operate extensive data centre networks and maintain significant operational footprints within the EU, a substantial share are not headquartered in the Union. This reflects the global nature of cloud and digital infrastructure markets, in which services critical to financial and other institutions are typically delivered through internationally integrated corporate and technological structures. This structural reality aligns with a recent report highlighting that Europe's reliance on non-EU technologies constitutes a strategic vulnerability: around 80 per cent of core digital technologies are imported, with cloud services representing one of the areas of highest dependency.[3]

The associated risks are often discussed in terms of market concentration. However, market concentration is not, in itself, the primary vulnerability. The more critical issue is that concentration can become durable because the market is insufficiently contestable, particularly where unfair or

[1] Examples of large-scale cloud outages in 2025 include incidents affecting AWS, Microsoft Azure, Google Cloud, and Cloudflare (major outages in November and December 2025).

[2] European Banking Authority. (2025, November 18). The European Supervisory Authorities designate critical ICT third-party providers under the Digital Operational Resilience Act [Press release]. Available at: https://www.eba.europa.eu/publications-and-media/press-releases/european-supervisory-authorities-designate-critical-ict-third-party-providers-under-digital. Also see: EBA. (2025). List of designated critical ICT providers. Available here: https://www.eba.europa.eu/sites/default/files/2025-11/e388451b-356b-408a-bbf2-b8e425865d75/List%20of%20designated%20CTPPs.pdf

[3] Kanclere, G.V., Eggert, M., and Skiotyte, G. (2026). European Software and Cyber Dependencies. PE 778.576 - December 2025. European Parliament. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2025/778576/ECTI_STU(2025)778576_EN.pdf.

anti-competitive practices, technical frictions, and contractual constraints limit effective choice. The key risk therefore emerges when high concentration coincides with structural barriers to choice and switching.

When portability, interoperability, multi-cloud deployment, or timely exit are not feasible without substantial cost and system re-engineering, diversification cannot be implemented quickly once disruptions occur. Lock-in is therefore not limited to Software as a Service (SaaS), but also affects Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), particularly where customers depend on proprietary managed services, tightly coupled identity and access controls, provider-specific observability tools, networking architectures, and data transfer conditions that raise the technical and economic barriers to migration or replication.

From this perspective, resilience and security risks do not arise solely from the technical or operational features of individual providers, but from structural market conditions that limit diversification and switching. These conditions are often created or reinforced by the behaviour of large providers, whose decisions on licensing terms, interoperability, and onboarding practices can shape options across the entire market. Where workloads are technically portable, organisations can plan for resilience in advance by diversifying across providers and adopting multi-cloud or failover architectures. By contrast, where portability is constrained by contractual, licensing, or architectural barriers, customers may be unable to distribute workloads meaningfully, and shared infrastructure can become a source of systemic fragility.

1.2 Market Adaptation and the Limits of Sovereignty

According to recent data from Synergy Research, enterprise spending on cloud infrastructure services reached USD 106.9 billion in the third quarter of 2025, reflecting the fastest sequential growth recorded to date. Year-on-year global cloud spending increased by 28 per cent, with public IaaS PaaS growing by around 30 per cent. Growth has been particularly strong in generative artificial intelligence-related services, such as Graphics Processing Unit as a Service (GPUaaS), which are expanding at annual rates exceeding 200 percent. Europe broadly mirrors these global trends.[4]

In Europe, cloud infrastructure revenues (including IaaS, PaaS and hosted private cloud services) reached approximately €36 billion in the first half of 2025, with full-year growth projected at around 24 per cent. While European providers have tripled their revenues since 2017, their combined market share has remained broadly stable at around 15 per cent since 2022, compared with roughly 70 per cent held by the three largest global providers. The fastest-growing European markets include Ireland, Spain and Italy, while the UK and Germany remain the largest markets

[4] Synergy Research (2025). Cloud Market Growth Rate Rises Again in Q3, Biggest Ever Sequential Increase. Available at https://www.srgresearch.com/articles/cloud-market-growth-rate-rises-again-in-q3-biggest-ever-sequential-increase.

by overall volume.[5] Estimates mapping cloud dependency (Table 1) point to both core cloud infrastructure and enterprise software layers, where reliance remains strong towards non-EU providers.

TABLE 1: MARKET DEPENDENCY MAPPING

Technology Domain	Sub-domain	Top 5 market concentration	Estimated EU providers' market share
Cloud Computing	Cloud infrastructure (IaaS / PaaS)	~80% (hyperscalers: AWS, Azure, etc.)	~13–15% (EU cloud firms combined)
	Cloud-delivered enterprise software (SaaS)	~65% (SAP, Oracle, Microsoft, Salesforce, IBM)	Over 20% (SAP among main vendors)
Enterprise Software	Productivity and Collaboration	~95% (Microsoft ~90%; Google rising)	<5% (limited opensource adoption)
	ERP	~85% (SAP ~55%; Oracle ~10%; others ~5–8% each)	¬70% (SAP plus mid-tier EU vendors)
	CRM	~75% (Salesforce dominant; next ~5–10% each)	~10% (SAP modest; no major EU CRM player)
	Server OS	~95% (Windows Server and Linux vendors)	No large EU OS vendor

Source: Kanclere, G.V., Eggert, M., and Skiotyte, G. (2026). Policy Department for Transformation, Innovation and Health Study on European Software and Cyber Dependencies

Current market practices therefore suggest that switching remains constrained in practice. In particular, long-term contracts and licensing arrangements reinforce lock-in by raising both the financial and operational costs of moving to alternative providers or architectures. These agreements often include mechanisms such as volume or spend commitments, automatic renewals, and significant early termination charges, which can make switching economically unattractive and thereby incentivise continuation of the status quo.[6]

Lock-in pressures can be further amplified through proprietary licensing and bundling strategies, where software components are packaged in ways that discourage substitution. In such cases, replacing one element of a software stack with an interoperable alternative may trigger licensing non-compliance, reduce entitlement to updates, or invalidate vendor support obligations. From a policy perspective, these practices are significant not merely because they reflect concentration,

[5] Synergy Research (2025). European Cloud Providers' Local Market Share Now Holds Steady at 15%. Available at https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15. Data Center Dynamics (2025). European cloud providers hold 15% of local market share. Synergy Research. Available at https://www.datacenterdynamics.com/en/news/european-cloud-providers-hold-15-of-local-market-share-synergy-research/. According to Synergy Research, among European providers SAP and Deutsche Telekom each hold around 2% of the market, followed by OVHcloud, Telecom Italia, Orange and a range of smaller regional players. Public IaaS and PaaS account for most of the market and continue to grow faster than hosted private cloud services, with GenAI offerings such as GPUaaS and GenAI PaaS expanding by 140–160% year-on-year. The UK and Germany remain Europe's largest cloud markets, while Ireland, Spain and Italy show the highest growth rates. The cloud market is a game of scale – requiring massive long-term investment and operational excellence.

[6] Kanclere, G.V., Eggert, M., and Skiotyte, G. (2026). European Software and Cyber Dependencies. PE 778.576 - December 2025. European Parliament. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2025/778576/ECTI_STU(2025)778576_EN.pdf

but because they can undermine contestability by narrowing realistic pathways for migration, multi-sourcing, and adoption of open alternatives.

Despite persistent structural barriers to switching, cloud users are increasingly diversifying their ICT architectures through multi-cloud strategies, open-source adoption (illustratively, in February 2023, the European Data Protection Supervisor (EDPS) launched a pilot project using open-source tools, including Nextcloud and Collabora Online (based on LibreOffice technology), to support secure file sharing, messaging, video calls, and collaborative document editing[7], and stronger emphasis on portability and interoperability. However, a key point is that portability cannot be treated as a substitute for reliability. Portability and interoperability reduce dependency and improve exit options, but they do not eliminate the need for operational resilience. Reliability must be established in advance, and, where appropriate, strengthened through proactive architectural choices such as multi-cloud deployment, redundancy, and tested failover, rather than being treated as a response mechanism after disruption has already occurred.

This is especially important given the rapid adoption of AI, because many AI workloads, models, and data pipelines are built and run on provider-specific cloud-native services (e.g., managed ML platforms, data orchestration, IAM/security, monitoring, and proprietary integrations).[8] Over time, this can increase switching costs and lock-in risk, since migrating often requires rewriting pipeline logic, replacing service dependencies, moving large volumes of data, and revalidating performance and reliability. While some teams mitigate this by using portable approaches such as containers, Kubernetes, open-source frameworks, and cross-cloud tooling, data gravity and operational coupling can still make switching providers costly and complex.

Survey data points to growing interest in regional deployment options and hybrid and multi-cloud configurations, alongside continued rapid global market expansion.[9] This is particularly relevant given that, while the internet was originally designed as a decentralised and resilient network, today's cloud ecosystem has evolved into a more concentrated ownership structure, with a large share of digital activity controlled by a limited number of providers. In such an environment, even localised disruptions can have wide-ranging effects.[10]

Interest in "local" or "sovereign" cloud solutions does not automatically increase resilience. Full independence from global cloud ecosystems would require sustained investment and may conflict with the need for globally sourced threat intelligence, advanced security tools, and AI-driven detection. For many organisations, resilience therefore depends less on disengagement

---

7 European Data Protection Supervisor. (2023). EDPS launches pilot to use open-source software in its IT environment. Available at: https://www.edps.europa.eu/press-publications/press-news/press-releases/2023/edps-pilot-use-open-source-software_en.

8 Blancato, F. G. (2023). The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem. Policy & Internet. Available at: https://doi.org/10.1002/poi3.358.

9 Gartner (2025). Gartner Survey Reveals Geopolitics Will Drive 61% of CIOs and IT Leaders in Western Europe to Increase Reliance on Local Cloud Providers. Available at https://www.gartner.com/en/newsroom/press-releases/2025-11-12-gartner-survey-reveals-geopolitics-will-drive-61-percent-of-cios-and-information-technology-leaders-in-western-europe-to-increase-reliance-on-local-cloud-providers.

10 Remarks made by Rob Jardin, chief digital officer at cybersecurity firm NymVPN in Valinsky, J. (2025, October 20). The internet just had another global outage. Why does this keep happening? CNN Business. Available at: https://edition.cnn.com/2025/10/20/tech/aws-why-internet-outages-keep-happening#:~:text=%E2%80%9CThe%20internet%20was%20originally%20designed,impact%20is%20immediate%20and%20widespread.%E2%80%9D.

than on layered architectures that improve transparency, redundancy, and governance while maintaining access to global innovation.

Resilience therefore depends less on provider numbers or location than on the ability to adapt architectures, switch suppliers, and deploy appropriate tools as operational, security, or geopolitical conditions evolve. This understanding has important implications for how regulatory, competition, and cybersecurity policies are designed and calibrated. Whether concentration translates into dependency is determined less by market shares than by lifecycle choices. Dependencies are often created at the point of onboarding, when architectural, licensing, and tooling decisions narrow future options, and revealed at the point of exit, when organisations attempt to migrate or recover under stress. The sections that follow examine resilience and security through this lifecycle perspective.

Against this background, **Section 2** clarifies how resilience and security are defined across business, regulatory, and competition communities, and shows that these perspectives converge on structural and lifecycle drivers rather than purely technical metrics or market shares. **Section 3** translates these concepts into operational mechanisms, examining how lifecycle constraints emerge in practice – first through restrictive licensing practices, and then through technical architectures and regulatory design choices that affect real portability, interoperability, security tool integration, and exit feasibility. **Section 4** draws the policy implications, assessing how competition enforcement, regulatory calibration, and public procurement can strengthen resilience by preserving adaptability, technological diversity, and access to global cloud innovation, while avoiding counterproductive fragmentation or prescriptive technological steering.

2. Definitions of Resilience and Security

This section examines how resilience and security are defined across business organisations, standards bodies, regulatory authorities, and competition agencies, and why these definitions matter for policy design. The objective is not to compare terminology, but to identify whether these institutions converge on a common understanding of what ultimately determines operational resilience in cloud environments.

Across these communities, a consistent pattern emerges: resilience is not treated primarily as a technical attribute of individual systems or providers, but as a structural property shaped by system architecture, governance arrangements, market structure, and contractual control. This matters because cloud infrastructure now underpins newer and evolving forms of infrastructure services across sectors, raising questions of dependency and concentration that affect both national security and operational risk.

These definitional differences are not merely academic. How resilience is defined therefore directly influences which policy tools are prioritised. Narrow technical framings tend to favour compliance rules, certification schemes, and provider-level safeguards. Structural framings instead focus on system design, portability over time, and whether organisations can freely

choose a cloud provider and retain practical exit options as part of ex ante resilience planning, (a detailed overview of definitions is provided in **Annex I**).

Across business users, standards bodies, cybersecurity authorities, and competition agencies, there is strong convergence on the core characteristics of resilience. Resilience is consistently understood as a structural property of digital systems rather than a purely technical attribute of individual technologies or providers. Common elements include architectural flexibility, effective governance and oversight, the capacity to absorb and recover from disruption, and the preservation of credible exit and recovery options. Although expressed in different vocabularies, these elements map onto distinct stages of the system lifecycle: design and onboarding decisions determine architectural flexibility and tool choice; operational governance shapes oversight and recovery capability; and exit conditions determine whether substitution, migration, or diversification remains feasible under disruptions.[11]

Differences arise primarily in emphasis rather than in underlying objectives. Business groups and competition authorities focus more explicitly on contractual constraints, licensing practices, and switching barriers that shape multi-cloud options and exit feasibility and the economics of redundancy. Cybersecurity authorities place greater weight on architectural autonomy, lifecycle security, and systemic risk management during operation and incident response.[12] Standards bodies adopt more neutral, technical language, prioritising continuity, adaptation, and shock absorption across interconnected systems. Despite these different entry points, all perspectives converge on the importance of maintaining adaptability across the full lifecycle of cloud deployment, including where public authorities procure services for sensitive workloads.[13]

A further point of convergence is caution against equating resilience with technological or geographic sovereignty. While jurisdictional exposure and geopolitical risk are widely recognised, the prevailing analytical view is that resilience depends less on ownership or location than on how systems are designed, governed, and interconnected in practice over time. This further underscores that digital sovereignty can differ in form and in practice: local hosting and "EU-based" provision may strengthen control in some respects, but they do not necessarily eliminate reliance on external infrastructure or enabling services.

In practice, even providers presented as privacy-focused or "sovereign" may frequently remain dependent on underlying components such as hyperscale infrastructure layers, content delivery networks, DDoS mitigation services, and third-party DNS resolution. These layered dependencies are material for both operational resilience and sovereignty assessments, because they may shape failure points, recovery pathways, and exposure to non-EU legal or technical control. Many services, including core enterprise functions such as email, collaboration, and identity, therefore

---

[11] Cigref (2022). Cigref publishes its second version of the trusted cloud reference document. Available at: https://www.cigref.fr/cigref-publishes-its-second-version-of-the-trusted-cloud-reference-document#:~:text=This%20version%202%20of%20the,the%20environmental%20footprint%20of%20cloud.

[12] Enisa. (2023). Cloud Cybersecurity Market Analysis. Available at: https://www.enisa.europa.eu/sites/default/files/publications/Cloud%20Cybersecurity%20Market%20Analysis.pdf.

[13] BSI and ANSSI (2025). Joint Statement by ANSSI and BSI on Cloud Sovereignty Criteria. Available at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/ANSSI-BSI-joint-releases/Cloud-Sovereignty-Criteria.html.

combine European-facing offerings with globally operated infrastructure or critical enabling services that sit outside the direct governance scope of the end user.

The policy implication is that resilience is best strengthened through enforceable conditions that preserve architectural choice, portability, and credible multi-cloud options across the full lifecycle, rather than through restrictive localisation or ownership requirements that may leave the underlying points of dependency unchanged. In other words, resilience is most effectively advanced by reducing structural barriers to switching and ensuring interoperability at the infrastructure and platform layers, not simply by relocating workloads within the EU.

Taken together, these instruments signal a regulatory shift towards treating resilience as a systemic and lifecycle challenge. However, whether these objectives are effectively translated into regulatory design is less clear. As the analysis below shows, horizontal obligations and uniform technical requirements can still shape architectures, onboarding choices, and exit options in ways that risk reinforcing dependency rather than reducing it. Strengthening resilience therefore requires not only the right policy objectives, but proportionate, technologically informed instruments that preserve openness, interoperability, and competitive choice across the lifecycle.

3. RESILIENCE AND SECURITY AS CLOUD LIFECYCLE MANAGEMENT

Resilience and security are shaped by how cloud services are chosen, configured, and integrated in practice. Concepts such as portability and recoverability only become real through concrete design and contractual choices. Dependencies are therefore created primarily when organisations first adopt a cloud service and become visible when they later try to change provider or recover from disruption. For this reason, this section adopts a lifecycle perspective, focusing on how contractual and technical choices shape long-term flexibility and exit options.

3.1 How Cloud Service Models Shape Resilience

Different types of cloud services create dependency in different ways. When organisations use basic cloud infrastructure, dependency mainly arises from how networks, data storage, and system configurations are designed. Moving such systems later can be slow, costly, or technically difficult. When organisations use development platforms, dependency often arises because applications are built using provider-specific tools that do not easily work elsewhere. When organisations rely on ready-made cloud software, dependency tends to be embedded in data formats, workflows, and business processes that are difficult to transfer to competing services. Table 2 summarises where dependency typically emerges across cloud service models and how this affects practical exit and recovery. In all cases, these constraints are typically embedded during initial adoption and become visible only when organisations attempt to migrate, recover, or reconfigure under stress.

These differences explain why resilience cannot be assessed through a single technical metric. Each layer of the cloud stack creates distinct forms of lock-in with different implications for continuity, recovery, and switching. Using multiple providers can reduce some risks, but it also increases complexity and operational burden. Diversification strengthens resilience only when systems are deliberately designed and governed for flexibility. Operational resilience is therefore defined by the ability to continue operating during disruption and to adapt when conditions change. Concentration alone does not necessarily create fragility. Lock-in alone can already undermine resilience. Systemic risk emerges when concentration coincides with restricted exit and switching costs.

The next section examines how licensing practices shape this interaction. Detailed technical illustrations are provided

TABLE 2: HOW DIFFERENT CLOUD SERVICES CREATE DEPENDENCY AND AFFECT RESILIENCE

Cloud service type	What organisations mainly use it for	Where dependency typically arises	What becomes hard to change later	What this means for resilience
Infrastructure services (IaaS)	Running virtual servers, storage, and networks	System configuration and network design choices made at the start	Moving entire systems to another provider or back in-house can be slow, costly, and technically complex	Recovery is possible but may take time and significant effort; large migrations are difficult under pressure
Platform services (PaaS)	Building and running custom applications	Use of provider-specific development tools and platform features	Rewriting applications to work on another platform can require major redevelopment	Switching becomes costly and slow, reducing flexibility during incidents or market changes
Software services (SaaS)	Using ready-made business software (email, CRM, collaboration tools)	Data formats, workflows, and business processes embedded in the software	Transferring data and processes to another provider can be incomplete or disruptive	Substitution is difficult; operational continuity may depend heavily on one provider

Source: ECIPE

3.2 The Impact of Restrictive Licensing on Resilience and Security

Across all service layers, licensing practices are the primary mechanism through which exit and switching are constrained in practice. Crucially, licensing-related lock-in can occur even prior to cloud adoption. When migrating from on-premise environments, customers may be deterred from selecting competing cloud providers if doing so entails substantial licensing uplifts or mark-ups, thereby shaping provider choice from the outset. Market concentration in cloud and software services is often treated as a proxy for systemic risk. Concentration alone, however, does not determine resilience outcomes. What matters is whether customers retain the practical ability to switch providers, diversify deployments, and reallocate workloads as

conditions change. Licensing sits at the centre of this distinction. It shapes resilience twice – first by constraining what can be deployed and integrated at onboarding, and later by determining whether workloads can be duplicated, migrated, or recovered during disruptions or operational pressure.

Licensing practices may contribute to market concentration, but their more significant effect is limiting contestability – making it difficult for competitors to challenge incumbent providers once concentration has emerged. Where customers can move workloads, deploy independent tools, and maintain credible multi-cloud strategies and viable exit options, even highly concentrated markets can remain resilient. Structural fragility emerges when licensing frameworks make adaptation prohibitively costly, technically impractical, or contractually restricted. In this sense, restrictive licensing converts scale into dependency.

This dynamic is often underestimated because cloud contracts appear voluntary. In practice, committed-spend agreements, bundled discounts, and incentive structures progressively narrow real choice once workloads and operational processes become embedded. Decisions that appear commercially efficient at procurement can later become binding constraints during disruption or migration. Restrictions on licence mobility and bring-your-own-licence (BYOL) policies illustrate this effect. Software frequently cannot be reused across competing cloud platforms, forcing repurchase and sharply increasing switching costs. Dual-pricing models and vendor-specific metrics further raise the cost of multi-cloud operation, undermining redundancy and failover strategies for commercial rather than technical reasons. The result is structural lock-in that is often not reflected in market-share metrics, even though it is a key mechanism through which cloud service providers can strengthen and extend their market position, with direct consequences for resilience. From a resilience perspective, the relevant question is not whether alternatives exist in theory, but whether organisations can use them in practice when conditions demand it.[14]

The following section examines the main types of licensing restrictions and the mechanisms through which they constrain customer choice. Crucial to note is that they can constrain customer choices through distinct but overlapping mechanisms. Some restrict movement, others permit switching at prohibitive costs, whilst impose constraints through technical, contractual or compliance related means.

[14] OECD. (2025). Competition in the provision of cloud computing services. OECD Roundtables on Competition Policy Papers, No. 323. Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/05/competition-in-the-provision-of-cloud-computing-services_f42582ad/595859c5-en.pdf; also see: Jenny, F. (2023). Unfair Software Licensing Practices: A quantification of the cost for cloud customer. CISPE. Available at: https://cispe.cloud/website_cispe/wp-content/uploads/2023/06/Quantification-of-Cost-of-Unfair-Software-Licensing_Prof-Jenny_-June-2023_web.pdf

3.2.1 Restrictions Affecting Portability and Workload Mobility

These restrictions include BYOL prohibitions, limitations on licence mobility, and requirements to repurchase licences when migrating workloads. The resilience implications are direct: when licences cannot be reused across cloud environments, organisations face contractual or economic barriers to maintaining parallel deployments for redundancy or rapidly shifting workloads during outages. This undermines standard disaster recovery strategies and increases dependence on a single provider's resilience posture. The literature consistently associates limited portability with longer recovery times and heightened exposure to provider-level failures.[15] Security risks arise in parallel. Concentrating workloads within a single ecosystem increases correlated failure risk and constrains the ability to diversify security tooling and controls. In addition, where access to extended security updates, enhanced patching, or critical support is tied to premium or cloud-specific licensing tiers, patch management decisions may be distorted, resulting in prolonged exposure to known vulnerabilities.

TABLE 3: RESTRICTIONS AFFECTING PORTABILITY AND MULTI-CLOUD USE

Type of license	Licence Restriction	Examples	How it works
Restrictions that limit portability and multi-cloud use	No-BYOL (Bring Your Own Licence)	Windows Server on AWS EC2 (Shared)	Use of "License Included" AMIs is mandatory; customer-managed keys are not supported on shared hardware.
	Restricted BYOL	Oracle Database on AWS	Licences may be brought but apply at a significantly less favourable exchange rate on AWS than on Oracle Cloud.
	Differential BYOL treatment (favouring own cloud)	Red Hat Enterprise Linux (RHEL)	BYOL is supported on customer-managed VMs, but native AWS or Azure RHEL offerings require licence-included subscriptions.
	Licence mobility prohibitions	Microsoft's "Listed Provider" Rule	Migration requires Licence Mobility through Software Assurance; standard perpetual licences cannot be used on these clouds.
	Forced re-purchase on migration	VMware (Broadcom) Perpetual to Subscription	On-premises VMware licences cannot generally be upgraded or transferred to cloud VMware services; migration to AWS or Azure requires repurchase of cloud licences.
	Cloud-exclusive features / optimisation unlocks	Oracle RAC (Real Application Clusters)	Oracle RAC enables multi-server high availability but is supported only on Oracle Cloud Infrastructure or specialised hardware, not on AWS or Azure.

Source: ECIPE

[15] A 2023 survey found that the three most common reasons organisations seek workload portability are disaster recovery and business continuity, cost savings, and overall resilience. Respondents also highlighted portability as a way to improve optimisation and efficiency, enabling better latency, performance, and scalability. See: Techstrong Research. (2023). Cloud Workload Portability. PulseMeter. Available at: https://www.linode.com/linode/en/documents/white-paper/2025/cloud-workload-portability-techstrong.pdf

3.2.2 Financial Restrictions that Increase Switching Costs

This category includes architecture-dependent pricing, dual-running penalties during migration, and proprietary licensing metrics that inflate effective capacity requirements on rival clouds. By raising the economic cost of switching, these mechanisms transform nominal customer preference into practical dependency, reducing organisational agility and introducing structural risk. Even where alternative environments exist, the cost of operating workloads in parallel or executing a migration can be sufficiently high that resilience plans become difficult to operationalise in practice, limiting timely responses to prolonged outages or sustained performance degradation. Security outcomes are similarly affected. Elevated switching costs can delay or constrain an organisation's ability to move workloads away from a provider experiencing a security incident, compliance failure, or deteriorating risk posture where doing so would trigger substantial additional licensing expenditure.

TABLE 4: RESTRICTIONS INCREASING SWITCHING COSTS

Type of license	Licence Restriction	Examples	How it works
Restrictions that increase switching costs	Architecture-dependent pricing (per-core inflation factors)	Oracle Cloud	Requires two licences per vCPU on AWS or Azure, but only one per vCPU on OCI.
	Dual-running / migration penalties	Oracle's general licensing rule and MSFT ESU programme	No dual-use grace period is provided during migration, requiring full licence payment for both on-premises and cloud deployments.
	Restrictive reassignment / movement rules	Oracle & SAP	Uses proprietary metrics (e.g. PVU), making licence requirements for containerised multi-cloud deployments unpredictable and often resulting in over-licensing.
	Unpredictable or punitive auditing regimes	Oracle & IBM	Often referred to as "audit bargaining": settlements convert audit exposure into cloud credits, locking budgets into expiring, vendor-specific commitments that restrict migration to rival providers.
	Misaligned License Metrics	VMware licensing (socket/core-based metrics vs native cloud vCPU measurement)	Uses proprietary metrics (e.g. vCPU), making licence requirements for containerised multi-cloud deployments unpredictable and often leading to over-licensing.

Source: ECIPE

3.2.3 Constraints on Interoperability and Integration

Vendors often constrain interoperability by delaying product certification on rival clouds, withholding technical specifications or APIs, or relying on proprietary interfaces. Because modern resilience increasingly depends on automation and coordinated operation across heterogeneous environments, such constraints limit the feasibility and reliability of multi-cloud architectures and impede the automation of failover and recovery processes. As a result, recovery operations tend to become slower, more manual, and more error-prone due to reliance on proprietary interfaces and uncertified configurations. Security outcomes are similarly affected. Reduced interoperability undermines defence-in-depth by limiting the deployment of layered security controls, restricting cross-environment log correlation, and constraining the use of independent monitoring, detection, and forensic tools.

TABLE 5: RESTRICTIONS AFFECTING INTEROPERABILITY

Type of license	Licence Restriction	Examples	How it works
Restrictions that constrain interoperability	Denial or delay of certification on rival clouds	SAP HANA	Delayed certification of high-performance configurations on AWS/Azure restricts access to best-in-class hardware and drives customers toward the vendor's preferred cloud.
	Withholding essential interoperability information	Azure SQL, Cloud SQL	A PaaS vendor restricts access to granular APIs required by third-party cloud management platforms to accurately report licence usage.
	Proprietary APIs that break portability	Azure Backup/ Recovery Services	Use of proprietary cloud-native backup and DR tools ties data and recovery processes to cloud-specific APIs and formats, impeding portability to other providers.
	Blocking integration with third-party tools	Entra ID/Azure AD	Core applications support only the vendor's identity provider, limiting integration with third-party IdPs and degrading single sign-on functionality.

Source: ECIPE

3.2.4 Commercial and Pricing Arrangements with Structural Effects

Some limitations on customer choice arise from pricing structures such as bundled discounts, loyalty incentives, and spend-commitment contracts that encourage deeper reliance on a single provider's ecosystem. These arrangements are not, in themselves, evidence of competitive harm. Nevertheless, where bundled discounts are attached to products with strong market positions, they may weaken incentives to diversify or switch, thereby reinforcing dependency over time. The resilience implications are structural: economic incentives often make maintaining parallel or secondary environments difficult to justify, encouraging consolidation and tying continuity planning to the resilience posture of a single provider. From a security perspective, these arrangements frequently concentrate core identity, access management, and security services within the dominant ecosystem. This reduces architectural diversity, increases reliance on vendor-specific security controls, and amplifies systemic risk through correlated failure.

TABLE 6: PRICING AND COMMERCIAL RESTRICTIONS

Type of license	Licence Restriction	Examples	How it works
Restrictions tied to pricing and commercial terms	Cloud infrastructure-linked software restrictions	Microsoft	Full functionality of dominant enterprise software is tied to the customer using the vendor's own IaaS (rather than other IaaS providers), increasing switching costs and limiting multi-cloud choice.
	Pricing discrimination: same licence, different cloud = different price	Microsoft licensing for workloads on AWS or Google Cloud instance	The software vendor's licensing imposes an additional surcharge (e.g. 15–20%) when the software is run under BYOL on non-preferred cloud environments (e.g. AWS or Google Cloud).
	Loyalty or spend-commitment discounts that deter multi-cloud	AWS Committed Use Discounts (CUDs) or Azure Enterprise Agreements (EAs)	Enterprise Agreements or Committed Use Discounts offer substantial discounts (e.g. 40%+) in exchange for multi-year, high-spend commitments across services.
	Identity/security layer bundling	Google Cloud IAM or Azure Entra ID	Requires use of the vendor's native IAM and KMS for database authentication, complicating deployment of the application layer on other clouds.

Source: ECIPE

3.2.5 Direct Restrictions on Security and Resilience Support

Certain licensing practices directly affect the level of technical support and the availability of security updates on rival clouds, including reduced support tiers, delayed patch delivery, and the revocation of disaster recovery rights following migration. The resilience implications are material: organisations operating outside the preferred environment may experience slower incident response and reduced ability to maintain equivalent failover or recovery capabilities. Security risks are correspondingly elevated. Unequal access to patches or extended security updates can result in prolonged exposure to known vulnerabilities, while restrictions on integrating external security tools further concentrate risk within a single vendor's ecosystem.

TABLE 7: SECURITY AND RESILIENCE RESTRICTIONS

Type of license	Licence Restriction	Examples	How it works
Restrictions that affect security and resilience	Support degradation on competitor clouds	Oracle Siebel or IBM WebSphere	Level 3 support on rival clouds is conditional on customers first demonstrating the issue is not caused by the underlying platform.
	Lifecycle / ESU discrimination (security updates differential)	Microsoft	Free Extended Security Updates are available only on Azure; other environments require a paid ESU subscription.
	Revocation of Secondary Use Rights on Rival Clouds	Microsoft (specifically on SQL Server and Windows Server passive DR rights) and Oracle (secondary use for testing/DR often requires full licensing)	Free passive DR rights under on-prem licences are revoked when the primary workload moves to a rival cloud, requiring full licensing of cloud-based DR.
	Proprietary Skill/ Certification Tying	AWS DynamoDB SageMaker	Proprietary certification and training requirements increase switching costs by tying skills investment to a single platform.
	Certified configurations" restricted to own cloud	SQL Server Managed Instance on Azure, or Cloud SQL for SQL Server on Google	High-end features requiring deep OS access (e.g. PolyBase, Stretch Database) are supported only on the vendor's specialised PaaS or VM offerings.

Source: ECIPE

3.2.6 Geographic and Compliance-Linked Restrictions

Some licensing conditions restrict where workloads may operate through region-locked licences or by limiting sovereign-cloud features to designated infrastructure. From a resilience perspective, these constraints reduce cross-border failover options and limit the ability to distribute risk across jurisdictions, increasing exposure to regional outages or geopolitical disruption. While such measures are often intended to support compliance objectives, they can create forms of "compliance lock-in" that constrain architectural flexibility, impede innovation, and hinder the adoption of multi-cloud security architectures capable of meeting regulatory requirements.

TABLE 8: GEOGRAPHIC AND REGULATORY RESTRICTIONS

Type of license	Licence Restriction	Examples	How it works
Restrictions connected to geographic or regulatory requirements	Region-locked licensing	Azure SQL, AWS RDS	Regional licence terms restrict PaaS databases and backups to specific regions, limiting cross-region DR and failover options.
	Access to sovereign / regulated-sector features only when using vendor's cloud	Azure Sovereign Cloud, Google Cloud Sovereignty Controls	Compliance-specific features are available only within the vendor's designated sovereign environment.

Source: ECIPE

In sum, these restrictions operate through three practical channels: they limit whether licences can move across environments; they raise the cost and risk of running systems in parallel during migration or recovery; and they constrain interoperability with alternative platforms and security tools. The cumulative effect is that exit remains formally possible but operationally slow, expensive, and risky – precisely when rapid adaptation is most needed.

3.3 Technology and Policy Constraints beyond Licensing

As demonstrated in earlier ECIPE work on cloud customer choice (CCC), barriers to exit are rarely contractual alone.[16] Licensing is the primary mechanism through which exit becomes restricted in practice, but it operates within a broader technical and regulatory environment that can either amplify or mitigate these constraints over the lifecycle. Architectural design choices, practical limits to portability, security tooling integration, and regulatory interventions all shape what can be onboarded, how systems evolve operationally, and whether credible exit and recovery remain feasible over the cloud lifecycle.

Because these constraints emerge through complex technical interactions that evolve rapidly and are often only partially observable even to domain experts, policy intervention must be calibrated carefully. Regulatory measures that directly prescribe technologies, architectures, or

[16] ECIPE (2025). Breaking Barriers to Cloud Customer Choice: Unlocking Europe's AI and Innovation Leadership. Available at https://ecipe.org/publications/unlocking-europes-ai-and-innovation-leadership/.

standards risk entrenching unintended dependencies, narrowing future design space, and locking in assumptions that may quickly become obsolete. The objective should therefore be to preserve adaptability across the lifecycle rather than to engineer specific technical outcomes.

3.3.1 Rights versus Real Portability

Regulatory initiatives such as the EU Data Act (DA) strengthen formal rights to switching and data access, but operational portability often remains limited.[17] Migrating live systems requires reconfiguring identity, networks, security controls, and application logic. For mission-critical workloads, engineering complexity, downtime risk, and compliance uncertainty frequently make migration slow or impractical. Exit constraints therefore originate in early architectural and onboarding choices, even where contractual rights exist. Portability that requires months of re-engineering offers little resilience in incidents measured in hours or days. This gap between legal entitlement and technical reality (described as the "Hotel California effect")[18] illustrates how exit constraints emerge from earlier onboarding and architectural choices: organisations can enter cloud ecosystems with relative ease, but once workloads are deeply embedded, exit becomes operationally impracticable.

Standardisation pressures can reinforce this effect. Where regulatory or compliance frameworks steer organisations towards uniform architectures to simplify oversight, they reduce architectural diversity and increase correlated risk. Over time, this can produce technical monocultures in which failures propagate more easily across organisations and sectors. From a resilience perspective, preserving practical exit and architectural diversity matters more than expanding formal switching rights alone.

3.3.2 Technical Architectures and Interoperability

Modern cloud environments increasingly rely on tightly integrated managed services, proprietary interfaces, and provider-native security models. While this improves efficiency and baseline security, it couples workloads closely to individual platforms and limits interoperability across identity systems, networking models, automation frameworks, and monitoring tools. Heterogeneous architectures can reduce correlated failure risk and support reconfiguration under stress, whereas highly standardised environments simplify compliance but concentrate systemic exposure (Table 9).

---

[17] Portability issues arise due to the lack of open interfaces. As a result, users face difficulties switching between services to obtain the best quality-to-cost ratio. Additionally, because of lack of interoperability between cloud services from different providers, these services cannot be easily combined either. See: Netherlands Authority for Consumers and Markets. (2022). Market Study Cloud services. Case no. ACM/21/050317 / Document no. ACM/INT/440323. Available at: https://www.acm.nl/system/files/documents/public-market-study-cloud-services.pdf.

[18] Concerns about cloud exit costs have often been framed against broader industry observations that storing very large datasets in public cloud environments can be substantially more expensive than equivalent on-premises infrastructure, and that data egress charges for repatriating large volumes of data may run into tens of thousands of pounds. Related evidence was submitted to the UK Competition and Markets Authority (CMA) during its Cloud Services Market Investigation. In Appendix O (Customer views on egress fees), a broadcaster described cloud egress fees as creating a "Hotel California" situation, where data can be moved into the cloud relatively easily, but exiting is operationally and economically difficult, and characterised both the cost of moving data out of the cloud and the use of multiple suppliers as "problematic". See: Appendix O: Customer views on egress fees. Available at: https://assets.publishing.service.gov.uk/media/67976c05cbd1e3a508a22c72/Appendix_O.pdf.

The use of proprietary APIs, identity and access systems, network security models, automation frameworks, and logging technologies across cloud providers undermines interoperability. This provider-driven heterogeneity forces a compartmentalised approach to multi-cloud security, increasing operational complexity and the risk of misconfiguration and emergent attack surfaces, even where individual platforms are secure in isolation.[19]

From a resilience perspective, architectural diversity can function as risk diversification.[20] Heterogeneous architectures reduce the likelihood that a single failure cascades across systems and providers and tend to rely more on provider-agnostic interfaces, supporting portability and reconfiguration under stress. By contrast, highly standardised architectures simplify oversight but concentrate risk: failures propagate more easily and workloads become tightly bound to proprietary hooks that constrain exit.

Importantly, these architectural interactions are highly complex and continuously evolving. Even specialist engineers rarely maintain full visibility across the entire dependency chain of modern cloud stacks. Regulatory efforts to prescribe specific technical architectures or standards therefore risk hard-coding incomplete assumptions and unintentionally narrowing future design options. Resilience is better supported by preserving flexibility and optionality than by mandating technical uniformity.

An illustrative example is France's ANSSI cloud sovereignty certification granted to S3NS, a joint venture between Thales and Google.[21] The model combines European governance, operational control, and access restrictions with continued use of Google's underlying IaaS and PaaS capabilities, including advanced data and AI services. Rather than replacing global infrastructure, resilience is achieved through layered architectural separation and governance controls, demonstrating how hybrid designs can reconcile sovereignty objectives with interoperability, scalability, and access to innovation.

---

[19] Duncan, R. (2020). A multi-cloud world requires a multi-cloud security approach. Computer Fraud & Security, 2020(5), 11-12, in Reece, M., Lander Jr, T. E., Stoffolano, M., Sampson, A., Dykstra, J., Mittal, S., & Rastogi, N. (2023). Systemic risk and vulnerability analysis of multi-cloud environments. arXiv preprint arXiv:2306.01862.

[20] A survey conducted by ENISA indicates that approximately 40 % of respondents identify secure cloud architectures including mobile, fog, and edge computing as priority research areas. This emphasis aligns with opportunities outlined in the EU report following the CEO roundtable "Shaping the next generation cloud supply for Europe," which highlights initiatives such as the cloud–edge continuum (e.g., hardware-based encryption at the edge), energy-efficient cloud infrastructures, cloud-native 5G, an open European ecosystem of cloud applications and toolkits, and greater convergence between information technology (IT) and operational technology (OT). The report also presents Secure Access Service Edge (SASE) as an opportunity for European providers, combining zero-trust network access, cloud access security brokerage (CASB), firewall-as-a-service, and data loss prevention into an integrated security model. See: ENISA. (2023). Cloud Cybersecurity Market Analysis. Available at: https://www.enisa.europa.eu/sites/default/files/publications/Cloud%20Cybersecurity%20Market%20Analysis.pdf ; also see: European Commission. (2021). European Commission. (2021). European industrial technology roadmap for the next generation cloud-edge offering. https://ec.europa.eu/newsroom/repository/document/2021-18/European_CloudEdge_Technology_Investment_Roadmap_for_publication_pMdz85DSw6nqPppq8hE9S9RbB8_76223.pdf

[21] Euractiv (2025). Google-backed cloud wins France's strongest sovereignty certification. Available at https://www.euractiv.com/news/google-backed-cloud-wins-frances-strongest-sovereignty-certification/.

TABLE 9: RESILIENCE IMPLICATIONS OF ARCHITECTURAL DIVERSITY AND STANDARDISED CONFIGURATIONS

Feature	Architectural Diversity	Standardised Configurations
Auditability	More complex; requires heterogeneous or custom checks	Easier; consistent controls enable repeatable audits
Systemic Risk	Lower; failures are less likely to propagate across environments	Higher; widespread reuse can enable correlated failures
Portability	Higher; often based on open or platform-agnostic standards	Lower; frequently relies on provider-specific abstractions
Operational Cost	Higher; demands broader expertise and tooling	Lower; benefits from operational consistency and automation

Source: ECIPE

3.3.3 Security Tool Integration and Resilience

A critical but often overlooked dimension of cloud resilience is whether organisations can onboard, integrate, and operate independent security tools alongside their cloud provider's built-in security services. Many organisations rely on third-party tools – such as monitoring systems, threat detection, identity management, encryption, and incident response software – to meet internal risk standards and regulatory requirements.[22] The ability to deploy and operate these tools reliably is essential for maintaining security and operational continuity during disruptions.

Provider-native security tools offer clear practical advantages. They are tightly integrated into the cloud platform and are easy to deploy and manage (Table 10). However, this convenience comes with structural trade-offs. Because these tools typically rely on the same underlying systems as the cloud platform itself, a provider outage, configuration error, or security incident can affect both the application and the security controls protecting it at the same time. Visibility is also limited to what the provider makes available, which can restrict independent monitoring across multiple cloud environments.

Independent security tools operate with greater separation from any single cloud platform. Although they often require more effort to integrate, they reduce shared points of failure and can continue operating even if parts of a cloud environment are disrupted. They also tend to provide broader visibility across systems and providers. From a resilience perspective, this separation enables layered protection and helps organisations maintain oversight and response capability during incidents.

The choice between convenience and independence is therefore not merely a technical decision, but a resilience-relevant design choice made early in the cloud lifecycle. Regulatory

[22] In fact, third-party cyber risk management (TPCRM) has emerged as a distinct discipline aimed at addressing the unique cyber risks introduced by vendor and supplier relationships. As third-party ecosystems expand, the external attack surface, including internet-facing assets, configuration weaknesses, and exposed data, has become an increasingly significant component of the overall threat landscape. See: Kost, E. (2025, June 15). TPCRM Framework: Building Digital Trust for Modern Enterprises. UpGuard. Available at: https://www.upguard.com/blog/tpcrm.

or procurement frameworks that implicitly favour vertically integrated security models risk reinforcing dependence on provider-native tools and discouraging independent alternatives. While integrated security can perform well under normal conditions, resilience depends on the ability to layer, substitute, and adapt security controls as risks evolve. Security tool choice is therefore not only a competition issue, but a core capability for operational continuity and recovery.

TABLE 10: RESILIENCE CHARACTERISTICS OF PROVIDER-NATIVE AND INDEPENDENT SECURITY TOOLS

Feature	Provider-Native Security	Independent (3rd Party) Tools
Integration	Tight, platform-native integration; low configuration overhead	Requires API integration and cross-platform configuration
Fate Sharing	Higher; availability typically tied to the cloud control plane	Lower; may operate partially out-of-band or across providers
Visibility	Constrained to provider-exposed telemetry and control points	Broader; can correlate signals across clouds and environments
Resilience	Strong within a single platform, but subject to correlated failures	Greater continuity during provider-specific outages

Source: ECIPE

3.4 Regulatory Design, Technological Diversity, and Lifecycle Lock-In

Several regulatory frameworks apply horizontal obligations across cloud services with limited differentiation between service layers, deployment models, or risk profiles. These include the EU Data Act, the NIS2 Directive, cloud certification schemes under the EU Cybersecurity Act, and elements of the DORA. While these instruments pursue legitimate objectives in security, resilience, and competition, their uniform application across heterogeneous cloud services creates important design tensions. Regulatory commitments shape not only how systems evolve operationally, but also which architectures organisations feel able to adopt at onboarding, narrowing future exit paths from the outset.

By favouring standardised compliance approaches, such frameworks can incentivise providers to converge on lowest-common-denominator service configurations in order to reduce regulatory uncertainty. In practice, this can limit the availability of specialised cloud environments for sensitive or mission-critical workloads and discourage integration with independent applications

and security tools.[23] As a result, organisations face fewer architectural options at onboarding and fewer viable alternatives later when they need to adapt, migrate, or recover from disruption. Portability may exist in legal terms, but switching becomes slow, costly, or operationally risky.

Similar risks arise when regulatory logic developed for public digital platforms or telecommunications infrastructure is applied to cloud services. Instruments such as the Digital Services Act (DSA) and, in parts, the Digital Markets Act (DMA) were designed for consumer-facing platforms, while proposals to extend telecom-style regulation under the European Electronic Communications Code (EECC) to cloud services have raised concerns about regulatory fit.

Imposing telecom-style obligations on cloud and content delivery networks (CDNs) would have significant systemic effects. Telecommunications operators that currently interconnect with cloud and CDN providers largely through domestic peering arrangements would increasingly need to do so at an international level or rely more heavily on transit. Moving away from efficient peering models would likely degrade performance, reduce resilience, and raise costs across the European internet ecosystem, affecting cloud and CDN providers, telecoms operators, and ultimately European businesses and consumers.[24]

Cloud environments support sensitive and mission-critical workloads and depend on differentiated architectures, controlled access, and layered security designs. Obligations aimed at openness, uniform treatment, or extensive disclosure would narrow the range of deployable architectures and discourage specialised configurations and third-party integrations.[25]

From a lifecycle perspective, these effects compound over time. Early onboarding and design choices become increasingly difficult to reverse. Architectural diversity diminishes. Credible exit options narrow as systems mature and dependencies accumulate. What appears to simplify compliance at the point of adoption can translate into structural lock-in when organisations later seek to switch providers, diversify architectures, or respond to incidents. Public procurement frameworks increasingly shape onboarding choices for critical workloads. Embedding

---

[23] CERRE, for example, notes that the absence of common cloud standards does not reflect a lack of technical proposals, but rather the difficulty of capturing the diversity, specialisation, and rapid evolution of cloud services within a single standard. While mandatory standardisation through regulation – such as interoperability requirements under the EU Data Act – may address incentives to favour proprietary solutions, it also risks locking providers and users into pre-defined standards. If applied broadly across service types, such mandates may reduce architectural diversity, constrain innovation, and limit differentiated service implementations (including security tools), with potentially adverse effects on both competition and resilience. See CERRE (2024). Competition and Regulation of Cloud Computing Services: Economic Analysis and Review of EU Policies. Available at https://cerre.eu/wp-content/uploads/2024/02/REPORT.CERRE_.FEB24.CLOUDS.pdf.

[24] Abecassis, D., Ryder, C., William, N., Lechner, L., and Bratty, R. (2024). The European telecoms regulatory framework: not a good fit for the public cloud. Analys Mason. Ref: 658783197-372. Available at: https://www.analysysmason.com/contentassets/d9396955aeb44e7a9898c809a884d69e/analysys-mason-report-for-aws---cloud-and-telecoms-regulation---final---2024-09-25.pdf

[25] Analogies between cloud services and telecommunications infrastructure risk obscuring a critical distinction. The Commission's White Paper reflects two related ideas: first, that legacy telecommunications regulatory models might be extended to cloud and digital services; and second, that convergence between networks and cloud infrastructures justifies this extension. However, proposals to extend the European Electronic Communications Code (EECC) to cloud and digital services have already met with resistance. Consultation results indicate that a majority of respondents (54.3 percent) opposed such an extension, reflecting concerns that telecom-style regulation is ill-suited to cloud markets. See European Commission. (2024). White Paper - How to master Europe's digital infrastructure needs? COM(2024) 81 final. Available at: https://digital-strategy.ec.europa.eu/en/library/white-paper-how-master-europes-digital-infrastructure-needs. Also see Stecher, T. M. (2024). Consultation on the EU's future connectivity networks: (Again) No support for regulatory intervention. DISCO. https://project-disco.org/european-union/consultation-on-eus-future-connectivity/ as referenced in Markevičiūtė, E. (2024, October 1). Bad ideas resurface: Expanding telco rules to digital and cloud and rebirth of "fair share". EU Tech Loop. Available at: https://eutechloop.com/bad-ideas-resurface-expanding-telco-rules-to-digital-and-cloud-and-rebirth-of-fair-share/.

portability and licensing neutrality at procurement stage therefore has disproportionate long-term resilience impact.

Autonomy policies follow the same logic. Efforts to expand European cloud capacity can strengthen resilience when they increase interoperable choice and architectural diversity. They risk weakening resilience when autonomy is interpreted as isolation or when national procurement and cybersecurity requirements prioritise location or ownership over portability and interoperability. National or regional solutions can reproduce the same lock-in dynamics if they rely on restrictive licensing, proprietary interfaces, or closed security architectures.[26]

Resilience is therefore strengthened not by technological uniformity or prescriptive regulation, but by preserving diversity, interoperability, and practical exit across the cloud lifecycle. Regulatory frameworks should remain cautious about directly steering technologies or standards in rapidly evolving and highly complex cloud ecosystems, where even technical experts rarely have full visibility over system interactions and long-term effects.

4. Conclusions: Resilience as a Lifecycle Property

This paper examined cloud concentration, resilience, and security through a pragmatic lens grounded in operational reality rather than abstract principle. The central conclusion is that resilience and security are lifecycle properties, shaped at two decisive moments:

1) Onboarding and deployment, when architectures, tools, licences, and integration choices are embedded; and
2) Exit and recovery, when organisations must adapt, migrate, or substitute providers under conditions of operational or security stress.

[26] Many critics of the proposed European Cybersecurity Certification Scheme (EUCS) have warned that if requirements extend beyond technical cybersecurity criteria into non-technical sovereignty or immunity clauses including restrictions based on supplier ownership, control, or location, they risk excluding otherwise legitimate providers and fragmenting the internal market. This concern is particularly salient in cloud computing, where infrastructure and services are continuously updated, scaled elastically, and modified without physical intervention. Further up the stack, software applications operate in an increasingly abstracted environment, unconstrained by the material safety certification regimes that govern physical goods, and subject instead to contractual, operational, and security assurances. While barriers to entry remain high at the level of hyperscale infrastructure, they are comparatively low at the application and service layers, where success depends less on regulatory compliance than on the ability to solve user problems effectively. Against this backdrop, proponents of the EuroStack initiative advocate a unified European alternative that collapses these heterogeneous layers into a single sovereignty-driven industrial project, often coupled with calls for exclusive or preferential EU-based public procurement. Critics argue that this "Airbus-style" model misconstrues the economics of digital markets by applying vertically integrated industrial policy logic to a modular, globally interdependent cloud ecosystem. See: Kilcoyne, M. (2025, August 22). Why the Airbus Model Won't Work for European Digital Policy. Center for Data innovation. Available at: https://datainnovation.org/2025/08/why-the-airbus-model-wont-work-for-european-digital-policy/; the resulting policy debate increasingly sits at the intersection of compliance and procurement. In this context, the Commission's October 2025 tender for sovereign cloud computing services valued at €180 million over six years and implemented through the Cloud III Dynamic Purchasing System (DPS) can be interpreted as an attempt to operationalise sovereignty concerns through procurement without imposing exclusionary eligibility rules. Rather than relying on binary notions of sovereignty, the Cloud Sovereignty Framework evaluates providers across a range of criteria, including legal, operational, and security requirements, supply-chain transparency, technological openness, and environmental considerations. While contested, this multi-criteria approach offers a potential template for Member State cloud procurement that seeks to balance resilience and autonomy objectives with competition, interoperability, and market openness, without resolving the deeper tensions inherent in cloud sovereignty policy. Its practical effects, however, remain uncertain. CISPE has argued that the framework's breadth and weighting may allow foreign hyperscalers to score as well as, or better than, European providers, raising concerns about whether it can meaningfully advance European cloud sovereignty in practice. See European Commission. (2025). Cloud Sovereignty Framework Version 1.2.1 – Oct. 2025. Available at: https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en; also see the following articles for references: Bomont, C. (2025, November 3). Technical is political: When a cloud certification scheme divides Europe. European Union Institute for Security Studies. Available at: https://www.iss.europa.eu/publications/briefs/technical-political-when-cloud-certification-scheme-divides-europe#endnote-005; Robinson, D. (2025, October 27). EU sovereignty plan accused of helping US cloud giants. The Register. Available at: https://www.theregister.com/2025/10/27/cispe_eu_sovereignty_framework/.

Across the analysis, a consistent pattern emerges. Many risks commonly attributed to market concentration do not arise from scale as such, but from constraints introduced early in the lifecycle that later narrow practical exit options. Where onboarding decisions embed restrictive licensing terms, proprietary interfaces, or tightly coupled operational dependencies, formal rights to portability and switching often remain theoretical when they are most needed. In these cases, resilience exists in principle but not in operational practice.

4.1 Technical Complexity and the Limits of Regulatory Intervention

A further insight from the analysis is that the technical foundations of cloud resilience are highly complex and continuously evolving, even for sophisticated private and public sector users. Modern cloud environments integrate runtimes, identity systems, security controls, automation frameworks, and operational processes in ways that are difficult to observe externally and challenging to standardise safely. Effective security and reliability emerge from tightly coupled engineering decisions accumulated over time.

For this reason, regulatory interventions that seek to prescribe specific technical architectures, interfaces, or configurations carry material risk. Measures that mandate uniform technical solutions can unintentionally weaken security, reduce architectural diversity, and increase correlated failure risk by encouraging technical monocultures. In environments supporting sensitive and mission-critical workloads, the consequences of regulatory over-specification are operational and security-relevant, not merely economic.

This does not imply regulatory inaction. It implies regulatory calibration and technological humility.

4.2 Licensing and Contracts as the Primary policy Lever

The analysis demonstrates that contractual and licensing practices constitute the most powerful and proportionate policy lever available to policymakers and competition authorities to improve reliability and security. Unlike deep technical architectures, licensing terms are observable, enforceable, and directly shape both onboarding choices and exit feasibility across the lifecycle. Licensing determines:

- which applications, tools, and security solutions can be deployed at onboarding;
- whether workloads can be duplicated, dual-run, or migrated during disruption;
- whether redundancy and failover strategies remain economically viable; and
- whether exit is operationally feasible rather than merely contractual.

Where licensing prevent portability, restricts licence mobility, inflates switching costs, or discriminates between functionally equivalent deployments across clouds, it creates dependencies that reinforce and increase market concentration. In such settings, concentration is not merely an observed market outcome but a mechanism through which customers become structurally constrained in their ability to diversify or switch providers. Conversely, licensing

frameworks that preserve reuse, mobility, and dual-running can support resilience, even in concentrated markets, by keeping diversification and exit options commercially and operationally credible.

From a policy perspective, licensing therefore represents high-impact, low-intrusion intervention space: adjustments here can materially strengthen resilience without destabilising underlying technologies or security architectures.

4.3 Implications for Competition Enforcement

Competition has an important role in supporting cloud resilience, but its focus should remain on contestability and lifecycle choice rather than market shares alone. A market can be concentrated and remain resilient if customers retain practical freedom to switch providers, diversify deployments, and integrate independent tools which can allow for low friction interoperability. Conversely, even structurally competitive markets become fragile when exit is constrained by contractual or licensing barriers. Such practices undermine not only competition but also operational resilience and continuity of security controls. Addressing them aligns competition enforcement with critical infrastructure protection and broader security objectives.

The CMA's recent assessment of certain software licensing practices was framed through the lens of whether these practices could lead to partial foreclosure in the market for cloud services. In particular, the CMA considered whether the licensing terms, either on their own or in combination with other market features, could prevent, restrict, or distort competition, for example by raising other providers' costs and limiting customers' ability to deploy software workloads on the cloud provider of their choice.

A key concern was that different cloud providers may be unable to adopt effective market access strategies to mitigate the competitive impact of a legacy software provider's licensing practices, particularly where customers face higher costs or contractual restrictions when running the provider's software on competing clouds.

The remedies considered during the investigation to address these concerns included:

- requiring non-discriminatory pricing for the relevant software products regardless of the cloud environment in which they are hosted;
- enabling customers to transfer previously purchased software entitlements to the cloud of their choice without incurring additional cost; and
- requiring parity in product availability and functionality when the legacy provider's software is used on third-party clouds compared with the provider's own cloud.

The non-discriminatory pricing remedy can in fact be understood as part of a broader obligation to license on fair, reasonable and non-discriminatory (FRAND) terms.[27] Importantly, it should

[27] Whelan, P. (2025). Software Licensing and the UK's Cloud Services Market Investigation: A Missed Opportunity to Remedy Anticompetitive Practices? Available at SSRN 5332643.

be noted that a FRAND-based approach does not necessarily imply price uniformity across all customers. Differentiated pricing and commercial terms may remain permissible where they are objectively justified.[28]

Competition authorities should therefore prioritise enforcement against:

- licensing terms that penalise dual-running or redundancy;
- discriminatory pricing or metrics that inflate costs on rival clouds;
- forced re-purchase of licences upon migration; and
- contractual practices that tie security, identity, or core functionality to a single ecosystem.

4.4 The Role of the EU Digital Markets Act (DMA)

The Digital Markets Act (DMA) could contribute in ways where it targets specific commercial practices that restrict choice, switching or interoperability. At the same time, this paper cautions against using the DMA as a broad instrument to reshape cloud technologies or architectures. Ongoing investigations on cloud computing services, including through investigations under Articles 17 and 19,[29] nonetheless leaves room for targeted enforcement aimed at removing commercial barriers to multi-cloud adoption, switching, and exit, while leaving technical design choices to market-driven innovation.

This distinction matters because the DMA was designed primarily with consumer-facing platform ecosystems in mind, whereas cloud services are predominantly enterprise inputs deployed in security-sensitive and compliance-intensive environments, where reliability, encryption, and operational resilience can shape purchasing decisions as much as price. Even so, the underlying competition concern is familiar: when switching becomes artificially costly, markets become less contestable. In cloud markets, these frictions often arise not from technical necessity but from commercial and contractual practices, such as disproportionate egress pricing, discriminatory licensing that penalises deployment on rival clouds, or proprietary coupling that limits interoperability and reinforces vendor lock-in.

Addressing these barriers can improve competitive pressure and customer choice. However, applying platform-style obligations indiscriminately risks unintended consequences, including:

- discouraging specialised or high-assurance cloud environments;
- narrowing architectural diversity and security tooling choice;
- incentivising lowest-common-denominator configurations; and
- substituting commercial portability remedies with one-size-fits-all technical mandates that may not work across diverse enterprise security requirements.

---

[28] Competition and Markets Authority. (2025, January 28). Cloud infrastructure services: Provisional decision report (Appendix W: Remedies appendix). Competition and Markets Authority, UK, p. 50. Also see: Competition and Markets Authority. (2025, July 31). Cloud infrastructure services: Final decision report (Appendix W: Remedies not taken forward in this market investigation). Competition and Markets Authority, UK, pp. 45–47.

[29] European Commission. (2025, April 23). Commission finds Apple and Meta in breach of the Digital Markets Act. Press corner. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2717

These risks could be mitigated if DMA enforcement focuses on enabling low friction customer-directed portability and interoperability, allowing organisations to retain their preferred architectures and security postures when switching or multi-sourcing.

The overarching policy lesson is that resilience is best supported through guidance and targeted policy measures rather than prescriptive technical intervention. Resilience should be understood as proactive: "exit during an outage" is rarely credible if organisations have not been able to build, test, and maintain viable alternatives in advance. The objective should therefore be to ensure that customers can select and combine the providers that best meet their needs before incidents occur, including through redundancy and multi-cloud strategies.

An important element of effective switching is also software equivalence. Where a supplier offers critical enterprise software across multiple cloud environments, customers should not face degraded security, performance, or functionality when running that software on rival clouds compared with the supplier's own platform. Ultimately, resilience is achieved by preserving credible exit over the lifecycle, the practical ability to reconfigure systems, substitute providers, and maintain operational and security continuity as conditions evolve.

Regulators and competition authorities can strengthen resilience by:

- preserving customer's contractual freedom to deploy, duplicate, and migrate workloads to the cloud provider of their choice;
- safeguarding the ability to onboard independent applications and security tools; and
- avoiding rules that implicitly favour technical uniformity over architectural diversity.

TABLE 11: SUMMARY OF POLICY FOCUS ACROSS THE LIFECYCLE

Policy focus area	Impact on onboarding and deployment	Impact on exit and recovery
Licensing portability and BYOL rights	Expands the range of deployable applications, tools, and architectures at entry	Enables duplication, migration, and failover without forced re-purchase
Restrictions on dual-running and redundancy	Discourages resilient architectures from the outset	Makes recovery during outages slow or infeasible
Technical openness mandates	Risk of weakening secure, specialised environments	Limited benefit if exit remains operationally impractical
Competition enforcement on contractual practices	Preserves choice and security tool diversity. Regulatory intervention may help ensure contestability at initial migration, before lock-in becomes structurally embedded.	Maintains contestability and credible exit
DMA-style technical obligations	Risk of narrowing architectural diversity	Risk of flattening exit options through standardisation

Source: ECIPE

REFERENCES

Abecassis, D., Ryder, C., William, N., Lechner, L., and Bratty, R. (2024). The European telecoms regulatory framework: not a good fit for the public cloud. Analys Mason. Ref: 658783197-372. Available at: https://www.analysysmason.com/contentassets/d9396955aeb44e7a9898c809a884d69e/analysys-mason-report-for-aws---cloud-and-telecoms-regulation---final---2024-09-25.pdf

AFME. (2021). Building Resilience in the Cloud. Available at: https://www.afme.eu/media/iddhw1kx/afmecloudcomputing202105.pdf

Appendix O: Customer views on egress fees. Available at: https://assets.publishing.service.gov.uk/media/67976c05cbd1e3a508a22c72/Appendix_O.pdf

Autorite de la concurrence. (2023). Cloud computing: the Autorité de la concurrence issues its market study on competition in the cloud sector. Available at: https://www.autoritedelaconcurrence.fr/en/press-release/cloud-computing-autorite-de-la-concurrence-issues-its-market-study-competition-cloud#:~:text=Finally%2C%20the%20Autorit%C3%A9%20observes%20that,can%20be%20mentioned%2C%20among%20others.

Blancato, F. G. (2023). The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem. Policy & Internet. Available at: https://doi.org/10.1002/poi3.358

Bomont, C. (2025, November 3). Technical is political: When a cloud certification scheme divides Europe. European Union Institute for Security Studies. Available at: https://www.iss.europa.eu/publications/briefs/technical-political-when-cloud-certification-scheme-divides-europe#endnote-005

BSI and ANSSI (2025). Joint Statement by ANSSI and BSI on Cloud Sovereignty Criteria. Available at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/ANSSI-BSI-joint-releases/Cloud-Sovereignty-Criteria.html

Business Europe. BusinessEurope's contribution to the Call for evidence on Cyber resilience act. Available at: https://www.businesseurope.eu/wp-content/uploads/2025/02/2022-05-24_cyber-resilience_act_-_reply_to_call_for_evidence-e1a-1.pdf

CERRE (2024). Competition and Regulation of Cloud Computing Services: Economic Analysis and Review of EU Policies. Available at https://cerre.eu/wp-content/uploads/2024/02/REPORT.CERRE_.FEB24.CLOUDS.pdf

Cigref. (2025). Geopolitics and Digital Strategy Challenges and levers for action for digital departments. Available at: https://www.cigref.fr/wp/wp-content/uploads/2025/03/Cigref_Geopolitics-and-Digital-Strategy_2025_EN.pdf

Cigref (2022). Cigref publishes its second version of the trusted cloud reference document. Available at: https://www.cigref.fr/cigref-publishes-its-second-version-of-the-trusted-cloud-reference-document#:~:text=This%20version%202%20of%20the,the%20environmental%20footprint-%20of%20cloud

CISPE. (2025). CISPE Sovereign Cloud Manifesto. Available at: https://cispe.cloud/website_cispe/wp-content/uploads/2025/07/Sovereignty-Manifesto-FINAL.pdf

CNCF. Cloud Native Security Whitepaper. Available at: https://www.cncf.io/wp-content/uploads/2022/06/CNCF_cloud-native-security-whitepaper-May2022-v2.pdf

Coalition for Fair Software Licencing. Coalition for Fair Software Licensing and Prescient Release Comprehensive Report Quantifying Link Between Restrictive Software Licensing and Cybersecurity Risks and Costs. Available at: https://fairsoftwarelicensing.com/wp-content/uploads/2023/12/Cyber-Report-Overview-2023.12.11.pdf;

Competition and Markets Authority. (2025, January 28). Cloud infrastructure services: Provisional decision report (Appendix W: Remedies appendix). Competition and Markets Authority, UK, p. 50.

Competition and Markets Authority. (2025, July 31). Cloud infrastructure services: Final decision report (Appendix W: Remedies not taken forward in this market investigation). Competition and Markets Authority, UK, pp. 45–47.

Data Center Dynamics (2025). European cloud providers hold 15% of local market share - Synergy Research. Available at https://www.datacenterdynamics.com/en/news/european-cloud-providers-hold-15-of-local-market-share-synergy-research/

Duncan, R. (2020). A multi-cloud world requires a multi-cloud security approach. Computer Fraud & Security, 2020(5), 11-12, in Reece, M., Lander Jr, T. E., Stoffolano, M., Sampson, A., Dykstra, J., Mittal, S., & Rastogi, N. (2023). Systemic risk and vulnerability analysis of multi-cloud environments. arXiv preprint arXiv:2306.01862

European Banking Authority. (2025, November 18). The European Supervisory Authorities designate critical ICT third-party providers under the Digital Operational Resilience Act [Press release]. Available at: https://www.eba.europa.eu/publications-and-media/press-releases/european-supervisory-authorities-designate-critical-ict-third-party-providers-under-digital.

EBA. (2025). List of designated critical ICT providers. Available here: https://www.eba.europa.eu/sites/default/files/2025-11/e388451b-356b-408a-bbf2-b8e425865d75/List%20of%20designated%20CTPPs.pdf

ECIPE (2025). Breaking Barriers to Cloud Customer Choice: Unlocking Europe's AI and Innovation Leadership. Available at https://ecipe.org/publications/unlocking-europes-ai-and-innovation-leadership/

Enisa. (2023). Cloud Cybersecurity Market Analysis. Available at: https://www.enisa.europa.eu/sites/default/files/publications/Cloud%20Cybersecurity%20Market%20Analysis.pdf

ENISA. (2023). Cloud Cybersecurity Market Analysis. Available at: https://www.enisa.europa.eu/sites/default/files/publications/Cloud%20Cybersecurity%20Market%20Analysis.pdf

Euractiv (2025). Google-backed cloud wins France's strongest sovereignty certification. Available at https://www.euractiv.com/news/google-backed-cloud-wins-frances-strongest-sovereignty-certification/

European Commission. (2025). Cloud Sovereignty Framework Version 1.2.1 – Oct. 2025. Available at: https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en

European Commission. (2025, April 23). Commission finds Apple and Meta in breach of the Digital Markets Act. Press corner. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2717

European Commission. (2024). White Paper - How to master Europe's digital infrastructure needs? COM(2024) 81 final. Available at: https://digital-strategy.ec.europa.eu/en/library/white-paper-how-master-europes-digital-infrastructure-needs

European Commission. (2021). European industrial technology roadmap for the next generation cloud-edge offering. https://ec.europa.eu/newsroom/repository/document/2021-18/European_CloudEdge_Technology_Investment_Roadmap_for_publication_pMdz85DSw6nqPppq8hE9S9RbB8_76223.pdf

European Data Protection Supervisor. (2023). EDPS launches pilot to use open source software in its IT environment. Available at: https://www.edps.europa.eu/press-publications/press-news/press-releases/2023/edps-pilot-use-open-source-software_en

European Commission. (2021). European industrial technology roadmap for the next generation cloud-edge offering. https://ec.europa.eu/newsroom/repository/document/2021

Gartner (2025). Gartner Survey Reveals Geopolitics Will Drive 61% of CIOs and IT Leaders in Western Europe to Increase Reliance on Local Cloud Providers. Available at https://www.gartner.com/en/newsroom/press-releases/2025-11-12-gartner-survey-reveals-geopolitics-will-drive-61-percent-of-cios-and-information-technology-leaders-in-western-europe-to-increase-reliance-on-local-cloud-providers

ITU. X.1051 : Information security, cybersecurity and privacy protection - Information security controls based on ISO/IEC 27002 for telecommunications organisations. Available at: https://www.itu.int/rec/T-REC-X.1051-202306-I/en

Jenny, F. (2023). Unfair Software Licensing Practices: A quantification of the cost for cloud customer. CISPE. Available at: https://cispe.cloud/website_cispe/wp-content/uploads/2023/06/Quantification-of-Cost-of-Unfair-Software-Licensing_Prof-Jenny_-June-2023_web.pdf

Kanclere, G.V., Eggert, M., and Skiotyte, G. (2026). European Software and Cyber Dependencies. PE 778.576 - December 2025. European Parliament. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2025/778576/ECTI_STU(2025)778576_EN.pdf

Kilcoyne, M. (2025, August 22). Why the Airbus Model Won't Work for European Digital Policy. Center for Data innovation. Available at: https://datainnovation.org/2025/08/why-the-airbus-model-wont-work-for-european-digital-policy/

Kost, E. (2025, June 15). TPCRM Framework: Building Digital Trust for Modern Enterprises. UpGuard. Available at: https://www.upguard.com/blog/tpcrm

Netherlands Authority for Consumers and Markets. (2022). Market Study Cloud services. Case no. ACM/21/050317 / Document no. ACM/INT/440323. Available at: https://www.acm.nl/system/files/documents/public-market-study-cloud-services.pdf

NIST. Cyber Resilience. Available at: https://csrc.nist.gov/glossary/term/cyber_resiliency

OECD. (2025). Competition in the provision of cloud computing services. OECD Roundtables on Competition Policy Papers, No. 323. Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/05/competition-in-the-provision-of-cloud-computing-services_f42582ad/595859c5-en.pdf

OECD. (2021). OECD Policy Framework on Digital Security. Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/oecd-policy-framework-on-digital-security_a0b1d79c/a69df866-en.pdf

Prasad, K., Fazal, A., Nimbalkar, K., & Amin, A. (2025, July). Quantifying EU public sector dependence on productivity software: A report for the Open Cloud Coalition. Open Cloud Coalition. Available at: https://opencloudcoalition.com/wp-content/uploads/2025/07/OCCEU-methodology-and-results-report.pdf

Prescient. Impact of Software Licensing Practices on Cybersecurity. Available at: https://fairsoftwarelicensing.com/wp-content/uploads/2023/11/Prescient-Cyber-Tax-Report-11.2023.pdf

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). PE/17/2022/REV/1

Remarks made by Rob Jardin, chief digital officer at cybersecurity firm NymVPN in Valinsky, J. (2025, October 20). The internet just had another global outage. Why does this keep happening? CNN Business. Available at: https://edition.cnn.com/2025/10/20/tech/aws-why-internet-outages-keep-happening#:~:text=%E2%80%9CThe%20internet%20was%20originally%20designed,impact%20is%20immediate%20and%20widespread.%E2%80%9D

Robinson, D. (2025, October 27). EU sovereignty plan accused of helping US cloud giants. The Register. Available at: https://www.theregister.com/2025/10/27/cispe_eu_sovereignty_framework/.

Stecher, T. M. (2024). Consultation on the EU's future connectivity networks: (Again) No support for regulatory intervention. DISCO. Available at: https://project-disco.org/european-union/consultation-on-eus-future-connectivity/ as referenced in Markevičiūtė, E. (2024, October 1). Bad ideas resurface: Expanding telco rules to digital and cloud and rebirth of "fair share". EU Tech Loop. https://eutechloop.com/bad-ideas-resurface-expanding-telco-rules-to-digital-and-cloud-and-rebirth-of-fair-share/

Synergy Research (2025). Cloud Market Growth Rate Rises Again in Q3; Biggest Ever Sequential Increase. Available at https://www.srgresearch.com/articles/cloud-market-growth-rate-rises-again-in-q3-biggest-ever-sequential-increase

Synergy Research (2025). European Cloud Providers' Local Market Share Now Holds Steady at 15%. Available at https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15

Techstrong Research. (2023). Cloud Workload Portability PulseMeter. Available at: https://www.linode.com/linode/en/documents/white-paper/2025/cloud-workload-portability-techstrong.pdf

UK Department for Science, Innovation and Technology. (2025). Cyber security and resilience policy statement. Available at: https://www.gov.uk/government/publications/cyber-security-and-resilience-bill-policy-statement/cyber-security-and-resilience-bill-policy-statement#:~:text=Resilient%20cyber%20infrastructure%20is%20essential,forefront%20of%20global%20technological%20advancements.

Whelan, P. (2025). Software Licensing and the UK's Cloud Services Market Investigation: A Missed Opportunity to Remedy Anticompetitive Practices? Available at SSRN 5332643.

ANNEX I – What each entity is thinking for resilience and security in context of cloud licensing restrictions (Note that this is not an exhaustive list. Definitions of resilience and security vary across entities, but they generally reflect the same core concepts).

Entity Grouping	Name	Definitions
Business Association	CISPE (Cloud Infrastructure Services Providers in Europe):	Defines resilience as the ability to maintain market choice and avoid vendor lock-in, viewing lock-in as a systemic security risk that threatens Europe's digital autonomy.
	CFSL (Coalition for Fair Software Licensing):	Links restrictive licensing to what it calls a "Cyber Tax": an unnecessary cost created by vendor lock-in that prevents businesses from investing in newer, more secure technologies, thereby undermining overall cyber resilience.
	CIGREF (Club Informatique des Grandes Entreprises Françaises)	Defines cyber resilience through the classic model of anticipating, withstanding, and recovering from major adverse cyber events.
	BusinessEurope	Organisations should treat modern, automated backup solutions not as secondary safeguards but as a foundational element of cybersecurity. The ability to rapidly restore systems to a trusted state, without paying ransoms or compromising data integrity, is framed not only as a cybersecurity essential but also as a key business differentiator.
	AFME (Association for Financial Markets in Europe):	Highlights regulatory concerns around concentration risk—the threat to financial stability and national security that arises when too many banks depend on a small number of cloud providers. AFME advocates for a balanced, risk-based approach to cloud adoption to mitigate these systemic vulnerabilities.
International Organisations	Cloud Native Computing Foundation (CNCF)	The CNCF defines a secure and resilient system as one built on loosely coupled, self-healing architectures that maintain integrity through the entire lifecycle, from code development (Shift-Left) to dynamic runtime environments. In this model, resilience provides the "operational security" by using declarative APIs and immutable infrastructure to automatically recover from failures or unauthorised changes, while security ensures that every layer of the "4Cs" (Cloud, Cluster, Container, and Code) is verified under a Zero Trust framework. Together, they transform security from a static perimeter into an automated, continuous process that allows applications to remain functional and trusted even when individual components are compromised or fail.
	OECD	Resilience will come from preparing and having a continued plan based on digital security risk assessment having it adopted, implemented and tested. In addition, resilience does not have a clear definition but allows information systems to carry on normal operations and resilience ensures business continuity and that one is prepared.
	ITU (International Telecommunication Union)	The ability of an organisation or system to maintain an acceptable level of service and security in the face of faults, attacks, or other adverse events by anticipating, absorbing, adapting to, and recovering from disruptions.

Entity Grouping	Name	Definitions
National Cybersecurity Agencies	BSI Germany	Defines cyber resilience as the ability of organisations and critical infrastructure to maintain and restore essential functions during and after cyber incidents by preparing for, withstanding, and recovering from disruptions. Its updated Technical Guideline TR-03183 Part 1 operationalises this through risk-based security measures and Security-by-Design/Default requirements aligned with the Cyber Resilience Act.
	NCSC UK	Defines cyber resilience in practice as the ability of the UK's critical systems and wider economy to withstand, respond to, and recover from advanced and common cyber threats. NCSC builds this resilience by delivering active cyber defence, shaping legislation and regulation, strengthening the national cyber ecosystem, and setting security standards for emerging technologies, drawing on intelligence from within GCHQ and its close partnerships across government, industry, and academia.
European Competition Authorities	Autorité de la concurrence	In its cloud-sector market study, the Autorité highlighted that emerging cybersecurity challenges and the rise of Large Language Models (LLMs) are developments likely to influence competition dynamics. It emphasised that competition authorities must ensure that dominant cloud providers ("hyperscalers") do not use these technological shifts to impede the growth of smaller or new entrants. This position implicitly links secure and resilient cloud services to competitive fairness, recognising that security and resilience can themselves become competitive parameters that must not be distorted by dominant actors.
	UK CMA	As the UK introduces its Cyber Security and Resilience Bill—expanding regulatory oversight to key digital service providers such as MSPs and data centres and imposing a stricter two-stage incident-reporting regime, the government positions resilient cyber infrastructure as essential for enabling innovation and supporting new technologies. Within this framework, the CMA's enforcement under the Digital Markets, Competition and Consumers Act (DMCCA) aims to promote fair competition in digital markets, which must operate on a secure and resilient foundation. This links the CMA's competition mandate to the wider objective of ensuring that digital market power is exercised in ways that do not undermine the resilience of the UK's digital ecosystem.

Entity Grouping	Name	Definitions
Standard Bodies	IEC	IEC TS 63074:2023, 3.1.6 defines cybersecurity of machine control systems as the set of activities necessary to protect the network and information systems, its users, and other affected persons from cyber threats, with respect to confidentiality, integrity, and availability. EN IEC 62443-3-2:2020 provides a framework for security risk assessment and system design in Industrial Automation and Control Systems (IACS), including identification of threats and vulnerabilities, calculation of likelihood and impact, specification of security level targets (SL-T) per zone/conduit, and post-mitigation evaluation of residual risk
	ISO	ISO 22316:2017 defines organisational resilience as an organisation's ability to absorb and adapt in a changing environment to deliver objectives and survive and prosper, emphasising anticipation, preparation, response, and adaptation. ISO/IEC 27001:2022 specifies requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS), with systematic risk assessment, governance controls, operational security measures, and continual improvement to support cyber resilience. ISO 22301:2019 specifies requirements for a Business Continuity Management System (BCMS) to ensure continuity of critical operations, effective response, and rapid recovery with minimal impact.
	NIST	The ability of an information system to continue operating under adverse conditions by maintaining essential operational capabilities, and to anticipate, withstand, recover from, and adapt to adverse events affecting systems that rely on cyber resources.