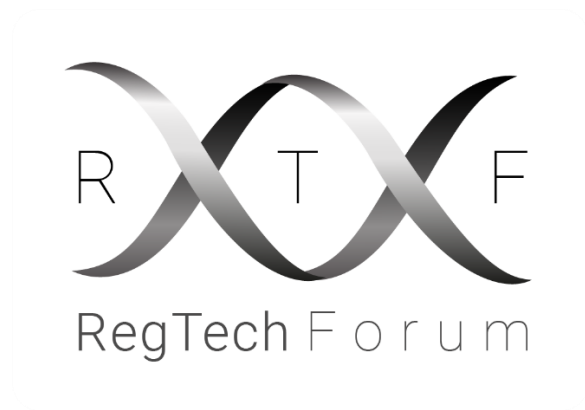




Cloud Sovereignty: The Need for a UK Sovereign Cloud

Devraj Basu¹ and Justin Field²

The demand for sovereign cloud, defined as a cloud environment entirely operated, located and governed within a country's borders, is accelerating worldwide, and the UK has become one of the most closely watched jurisdictions shaping this trend. This article provides a discussion of cloud sovereignty and then focuses on the issues around the development of a UK sovereign cloud, suggesting several solutions that would enable rapid and systematic development of a UK sovereign cloud.

1. Dimensions of Cloud Sovereignty

The EU has put forward its views on cloud sovereignty outlining eight criteria to achieve this in a given jurisdiction. We briefly review these, which they will form the basis of our analysis.

The eight criteria are:

- 1) **Strategic Sovereignty** which captures the degree to which the services of a cloud provider (or technology actor) are anchored within the jurisdiction's legal, financial, and industrial ecosystem. It assesses ownership stability, governance influence, and alignment with the jurisdiction's strategic priorities.
- 2) **Legal & Jurisdictional Sovereignty** which evaluates the legal environment, exposure to foreign authority, and enforceability of rights that govern the services of a technology provider. It determines the extent to which the services are anchored in the relevant jurisdiction and insulated from external legal claims.
- 3) **Data & AI Sovereignty** which focuses on the protection, control, and independence of data assets and AI services within the jurisdiction. It assesses

¹ Devraj.basu@strath.ac.uk

² Justin.field@blackboxhosting.co.uk

how data is secured, where it is processed, and the degree of autonomy customers retain over AI capabilities.

- 4) **Operational sovereignty** measures the practical ability of jurisdictional actors to run, support, and evolve a technology independently of foreign control. It focuses on continuity of operations, skill availability, and resilience against external dependencies.
- 5) **Supply chain sovereignty** evaluates the geographic origin, transparency, and resilience of the technology supply chain, focusing on the extent to which critical components and processes remain under the jurisdiction's control or is exposed to non-jurisdictional dependencies.
- 6) **Technology Sovereignty** evaluates the degree of openness, transparency, and independence in the underlying technological stack, ensuring jurisdictional actors can interoperate, audit, and evolve solutions without lock-in to foreign proprietary systems.
- 7) **Security & Compliance** sovereignty measures the extent to which security operations, compliance obligations, and resilience measures are controlled within the jurisdiction, ensuring independence from foreign jurisdictions and long-term operational assurance.
- 8) **Environmental sustainability** assesses autonomy and resilience of cloud services over the long term in relation to energy usage, dependency and raw material scarcity.

2. EU and UK Sovereign Clouds: State of Play

There appears to be growing awareness around issues of EU and UK sovereign cloud. In this section we will briefly review the current state of play based on the dimensions of sovereignty from the previous section.

Mario Draghi has proposed the establishment of an EU Cloud and AI Development Act³ to create a unified framework aimed at bolstering Europe's capabilities in high-performance computing, artificial intelligence, and quantum technologies. This initiative seeks to harmonize cloud architecture requirements and procurement processes across member states, fostering a more competitive environment for European businesses. Among other things, it seeks to define a single EU-wide policy and residency requirements for EU public administrations' cloud services as well as EU-wide sensitive data security policies for collaboration between private cloud providers and hyperscalers. This is designed to address the lack of a competitive EU-based offer of cloud computing services at sufficient scale to serve highly critical use cases with particularly high security needs, as found in various economic sectors and the public sector. A collection of European cloud CEOs has responded to the proposed Act by

³ <https://www.eu-cloud-ai-act.com/>

outlining five key principles and objectives they believe the Act should enable⁴, all of which fit within the dimensions of cloud sovereignty above. These are first, defining sovereignty by control, not EU presence or cybersecurity, second, ensuring operational autonomy where sovereign services are not available, third, reserved procurement shares for European providers for sensitive data and workloads, fourth, a cloud policy that reinforces competition and finally prioritizing the European ecosystem for taxpayer funded investments in cloud and AI infrastructure.

The drive for a UK sovereign cloud appears to be driven by three factors: First, regulation and compliance frameworks which fit with points 2), 3) and 7) from the previous section. The recently passed [Data \(Use and Access\) Act](#) strengthens the UK's data regime, emphasizing local data control and, in 2026, forcing firms to prioritize data residency to avoid legal pitfalls, thus ensuring security and compliance as well as data sovereignty. There are also the emerging issues around the US Cloud Act where US-based providers in the UK may be compelled to disclose data to US law enforcement undermining legal and jurisdictional sovereignty, making truly UK providers a preferred choice for high-sensitivity data. This fits within legal and jurisdictional sovereignty as well as data sovereignty. Second, geopolitics where global tensions have re-ignited questions about data dependency and foreign jurisdiction. This speaks to issues around strategic sovereignty emphasising the need for governance control within the UK and alignment with the UK's strategic priorities.

Consumer trust is the third factor providing impetus for a UK sovereign cloud. The operational, supply chain and technological factors 4), 5) and 6) are all important in this context. Data hosted, processed, and supported entirely within UK borders by UK-cleared personnel ensures that operational sovereignty is maintained and some sovereign providers are emerging⁵. Supply chain sovereignty was a major concern in the early days of UK cloud deployment⁶ but over time hyperscalers came to dominate with the UK based supply chain suffering as a result. However recent geopolitical developments as discussed above have led to an increasing demand for hosting critical workloads locally and partnering with sovereign providers.

The issue of technological sovereignty is crucial in this context, with the dominance of hyperscalers clearly inhibiting the growth of an indigenous UK cloud ecosystem. Proprietary technologies, lack of interoperability/portability standards and high switching costs (e.g., egress fees) deter customers from switching or using multi-cloud setups, leading to technological and commercial lock-in, reinforcing hyperscaler dominance. High barriers to entry and expansion with capital intensive infrastructure

⁴ https://www.cispe.cloud/website_cispe/wp-content/uploads/2026/03/Cloud-CEOs-Joint-Letter-March-17-2026-FINAL.pdf

⁵ <https://cyberfortgroup.com/> and <https://www.ans.co.uk/> for example.

⁶ <https://www.computerweekly.com/feature/Sovereign-cloud-and-AI-services-tipped-for-take-off-in-2026>

and economies of scale (data centres, network, operations) make it hard for smaller/cloud challengers to compete effectively. On the regulatory front, the UK's Data (Use and Access) Act aims to extend the Open Banking data access regime to other sectors and is not limited to any specific product or service category. The law is sector-agnostic and does not specifically address sharing and switching across cloud services, but this may evolve as secondary legislation is introduced.

3. The Competition and Markets Authority Cloud Market Investigation

The UK telecoms regulator Ofcom had identified potential competition issues in the UK cloud services market around technical barriers to setting up a multi-cloud architecture, fees connected with the transferring of data, discounts conditional on a certain amount of spend offered by certain cloud providers and software licensing practices. In response the UK Competition and Markets Authority (CMA) undertook a cloud market investigation with the final decision in July 2025⁷. Their final decision was that competition is not working well, with recommendations to address this. They found the market highly concentrated with the two largest providers, Microsoft and Amazon Web Services (AWS), having high market shares. Google had a much smaller market share, and other providers like Oracle and IBM have minimal market shares. Less than 1% of customers switch cloud providers and/or use multiple clouds, with most customers being “locked in” to their initial provider due to a combination of technical and commercial barriers. Smaller cloud providers were also disadvantaged by the need for substantial investment, the broad product portfolios of the three largest providers and the impact of economies of scale. Whilst AI related cloud services are growing, AI is not yet reshaping competition in the UK's cloud services market. The investigation recommended that the CMA Board use its digital markets powers to prioritise commencing SMS investigations to consider designating the two largest providers Microsoft and AWS with strategic market status (SMS) in relation to their respective digital activities in cloud services. This would enable the CMA to impose targeted and bespoke interventions to address the concerns we have identified, including with respect to features where there are specification risks around the design of effective market interventions.

Under the Financial Services and Markets Act 2023, HM Treasury can designate “critical third parties” supplying essential services to financial institutions, enabling regulators such as the Bank of England and Financial Conduct Authority (FCA) to scrutinise operational resilience and impose standards.

⁷https://assets.publishing.service.gov.uk/media/688b20e6ff8c05468cb7b120/summary_of_final_decision.pdf

4. The Hyperscaler Procurement Advantage for the UK Public and Private Sector

The [Open Cloud Coalition](#) (OCC), a collaborative advocacy group, promoting a diverse, competitive, and resilient cloud services industry across the UK, EU, and global markets argue public sector procurement frameworks and tenders often implicitly or explicitly favour dominant hyperscalers, raising barriers for smaller cloud firms. Complex tender processes with lengthy, complex bids and high past performance requirements disadvantage smaller providers lacking scale brand reputation. The OCC find evidence of entrenched contracts and single source deals suggesting long-term single-source public contracts with hyperscalers can further cement their position and reduce competitive re-evaluation. It is hard to quantify existing hyperscaler spend in UK public cloud spend, but existing evidence shows significant structural dependencies.

In the private sector context, the findings of the CMA report around less choice and higher costs could be costing UK organizations substantial amounts of money. As discussed in Section 2. Ofcom has reported that some hyperscalers are offering free credit worth millions of pounds to new businesses to secure their loyalty. This makes it difficult for smaller providers to compete and one that the regulator says pushes businesses into a proprietary ecosystem that precludes any possibility of a multi-cloud strategy. Indeed, several potential competitors such as UKCloud have been forced into liquidation or have had to pivot, possibly due to an unstated government preference for its hyperscale competitors at the expense of small providers.

In the context of the start-up sector, the dominant hyperscalers can lock-in early-stage start-ups with the offer of free credits as well as the offer of free courses. This creates a potential ecosystem dependency which could undermine supply chain sovereignty in key technological start-up ecosystems such as the AI and data sectors.

5 Suggested Solutions

The development of a UK sovereign cloud ecosystem should be seen both as a national security issue as well as an economic development issue. To that end, enabling the growth of smaller cloud providers plays a crucial role. The analysis below could help enable growth and development in this sub-sector.

We will discuss several suggestions that could enable the development of a sovereign UK cloud ecosystem. These suggestions may be classified into three groups, first, specific measures around reducing hyperscaler lock-in, second, building greater awareness around lock-in issues, thirdly enabling greater flexibility.

The first set of suggestions are a) **introduction of anti-lock in commercial rules** b) **cap or regulate egress fees** c) **cap credits**. The design and implementation frameworks for these rules are as important, if not more so, than their promulgation. The EU Data Act phases out cloud provider switching charges, including data egress fees, prohibiting them entirely by January 12, 2027. During a transition period (until early 2027), fees must be capped at costs directly related to switching, excluding overheads. This aims to increase multi-cloud adoption and data portability in the EU. It also mandates strict anti-lock-in rules for cloud providers, including IaaS, PaaS, and SaaS, to facilitate seamless switching. Key rules include mandatory contractual, technical, and commercial changes: eliminating egress fees by January 2027, enforcing a maximum two-month notice period, and requiring mandatory data portability support. Despite the elimination of egress fees, cloud switching rates in Europe barely budged. According to industry analysts, less than 3 per cent of enterprise workloads in 2024 moved between major cloud providers, roughly the same rate as before the announcements.

True lock-in comes from a web of technical dependencies, human capital investments, and business relationships that no regulation can easily unpick. Future regulations should tackle the root causes of lock-in: API incompatibility, proprietary service architectures, and the lack of meaningful standards. This might mean mandating open-source implementations of core services, requiring providers to support competitor APIs, or creating financial incentives for true interoperability. The credit economy creates its own form of lock-in. The hyperscalers aggressively court startups with free credits, for example AWS Activate offers up to \$100,000, Google for Startups provides up to \$200,000, and Microsoft for Startups can reach \$150,000. These credits come with conditions: they expire if unused, can't be transferred, and often require the startup to showcase their provider relationship. By the time credits expire, startups are deeply embedded in the provider's ecosystem.

The second set of suggestions are around risk assessment and management namely a) **encouraging cloud audits** and b) **encouraging lock-in risk assessments**. A cloud audit is a process that systematically reviews and assesses an organization's cloud infrastructure, security controls, and compliance posture. It is a comprehensive evaluation that examines the cloud provider's security practices, data access controls, and overall risk management strategies. The primary purpose of a cloud audit is to ensure that an organization's cloud environment meets industry-specific regulatory requirements, adheres to established security standards, and effectively mitigates potential risks. Cloud audits can be conducted by an independent third-party auditor or by an organization's internal audit team.

Cloud lock-in risk assessments evaluate the technical, financial, and operational dangers of over-reliance on a single cloud provider. The UK Government Digital Service

recommends⁸ monitoring the organization's cloud portfolio to identify situations early where the exit or switching costs could grow disproportionately as development continues. Monitoring should be carried out by a person or group responsible for the organisation's cloud strategy, for example a Cloud Centre of Excellence (CCoE). They recommend aiming to maximise both the value and portability of the services where possible. This could be achieved by having access to knowledge of a broad range of technical solutions, perhaps through a CCoE or architecture community. They also suggest bringing together procurement, financial and technology specialists to make collaborative decisions on cloud and to understand the advantages and disadvantages of the various kinds of cloud lock-in.

The final set of suggestions could be implemented via a combination of government actions, regulation and community best practices. These are a) **introduction of modular procurement** b) **vendor-neutral training** c) **mandated multi-cloud / portability requirements** and d) **requiring workloads to be deployable across two providers**. If government contracts required true portability, with regular switching exercises to prove it, providers would have enormous incentives to improve. The public sector, spending billions on cloud services, could be the forcing function for real interoperability and would help cloud SMEs grow.

Vendor-neutral cloud training provides foundational knowledge of cloud concepts, security, and architecture applicable across various providers (AWS, Azure, GCP) rather than focusing on one platform. There are several certifications which are ideal for multi-cloud environments, strategic roles, and building a broad, transferable skillset and are ideal for professionals seeking to understand the "why" and "how" of cloud architecture, security, and management rather than just the "where" of a specific vendor's interface.

The final two suggestions would likely require secondary legislation in the UK based on the Data (Use and Access) Act as pointed out in Section 2. Technical innovation could provide solutions where regulation falls short. Container technologies and Kubernetes have shown that some level of portability is possible. The next generation of abstraction layers potentially powered by AI that can automatically translate between cloud providers could make switching more feasible. Investment in these technologies should be encouraged through tax incentives and research grants.

For SMEs, the immediate solution isn't trying to maintain pure portability but building switching options into their architecture from the start. This means using cloud services through abstraction layers where possible, maintaining detailed documentation of dependencies, and regularly assessing the cost of switching as a risk metric. It's not about being cloud-agnostic but about being cloud-aware.

⁸ <https://www.gov.uk/guidance/managing-technical-lock-in-in-the-cloud>

6 Conclusion

Overall, the analysis illustrates how hyperscalers such as AWS and Azure create risk for the UK, both commercial as well as around national security. The rise of an SME ecosystem in the cloud space could help mitigate several of these risks and active Government policy and legislation could help enable this.

For example, [Black Box Hosting](#), a fast-growing UK cloud SME, provides a compelling alternative to public cloud models by directly addressing the sovereignty risks outlined in this paper. By delivering infrastructure that is fully UK-hosted, operated, and governed, they enable organisations to retain legal and jurisdictional control over their data, mitigating exposure to foreign legislation such as the US Cloud Act. This directly strengthens legal, data, and security sovereignty while ensuring compliance with evolving UK regulatory frameworks.

In contrast to hyperscaler environments, cloud SMEs such as BlackBox Hosting reduce the risk of vendor lock-in by prioritising transparent architectures, flexible, fixed price commercial models, and support for interoperable technologies. This enables customers to maintain greater control over their cloud strategy and budget, avoid punitive egress fees, and retain the ability to adapt or migrate as business and regulatory needs evolve.

Operationally, a UK-based provider ensures that support, skills, and infrastructure remain within the domestic ecosystem, enhancing resilience and continuity while contributing to the development of a sovereign supply chain. This not only reduces dependency on foreign-controlled platforms but also aligns with broader UK strategic and economic priorities by supporting local innovation and capability building.

Ultimately, choosing a provider such as BlackBox Hosting allows organisations to balance the benefits of cloud adoption with the need for control, transparency, and long-term resilience. In doing so, customers can significantly reduce the commercial, operational, and geopolitical risks associated with public cloud dependence, while contributing to the growth of a more competitive and sovereign UK cloud ecosystem.

