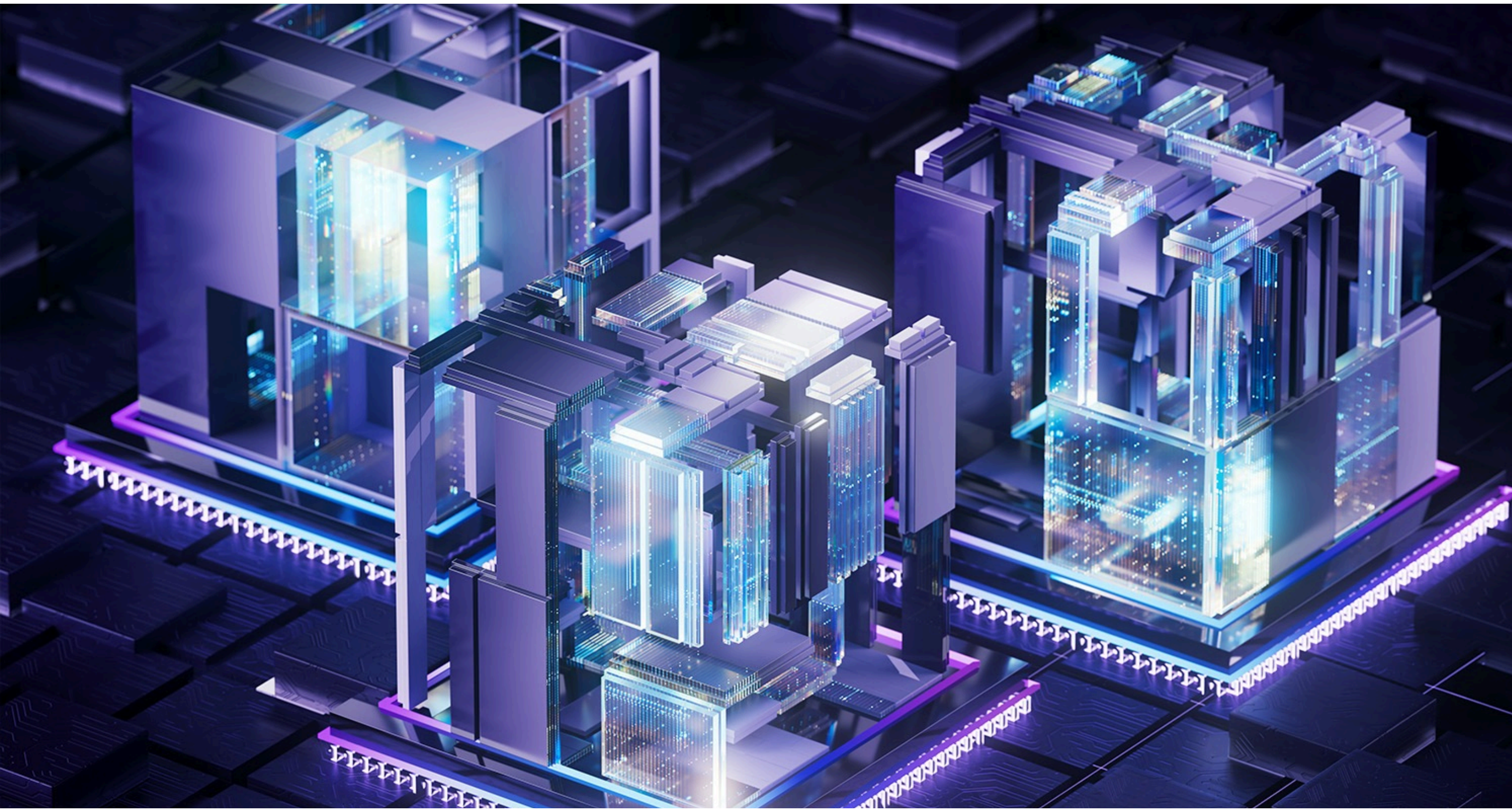
McKinsey & Company

McKinsey Technology

Boards are calling for more digital autonomy: How CIOs can deliver

A McKinsey survey of technology leaders shows that sovereignty concerns are shaping their IT investment choices. We present six strategies for CIOs to navigate the waters ahead.

by Arnaud Tournesac, Klemens Hjartar, and Matteo Martinelli
with Rossana Lo Re



November 2025

Almost every large company is grappling with how to adapt to a more fragmented and fast-changing geopolitical environment. Tariffs, regulatory shifts, and supply chain constraints are just a few of the obstacles that organizations must navigate. CIOs face a particularly complex challenge: They must manage risks tied to geopolitical uncertainty while also capturing the rewards of digital transformation such as faster innovation and cost efficiencies. Boards are calling for more technology sovereignty[1] while also pushing for rapid progress, causing CIOs to walk a tightrope. The discussion about how to balance sovereignty and innovation is deeply strategic and often starts in the boardroom, but it's the CIO who must take action in the machine room.

We recently surveyed more than 100 CIOs and other technology leaders in Europe, asking them which factors most influence their infrastructure choices—and technology sovereignty was at the top of the list. While the survey[2] focused on Europe, CIOs worldwide face similar challenges. Many CIOs seek to build tech autonomy and resiliency. They are looking for ways to reduce their reliance on global technology platforms to comply with regulations and ensure operational continuity. At the same time, they recognize the innovation benefits of these established providers.

Findings from our survey illustrate this dichotomy. Nearly half of European technology leaders whose companies do not use public clouds cite concerns about security and control of their infrastructure as the primary roadblocks. Even in organizations that do use public clouds, data security concerns—along with cost—are seen as barriers to scalability (exhibit). Yet CIOs realize these risks coexist with tangible benefits; global technology platforms provide innovation velocity, advanced capabilities, and economies of scale.

We identified six strategies that CIOs can deploy to enhance digital autonomy, strengthen resilience, and build a foundation for agentic AI innovation. These strategies aim to help organizations find their optimal position on the risk–reward frontier, balancing sovereignty and control against agility and innovation.

Five types of risk

Our work with multinational companies finds that nondiversified reliance on global technology platforms can increase resiliency risks in five main ways:

— **Regulatory complexity:** More-stringent national and regional data-protection laws are escalating scrutiny over where data resides, how it is processed, and who can access it. Laws with international scope such as the US CLOUD Act can introduce further compliance considerations, challenging the assumption that the region in which data physically resides maintains legal control over the data.

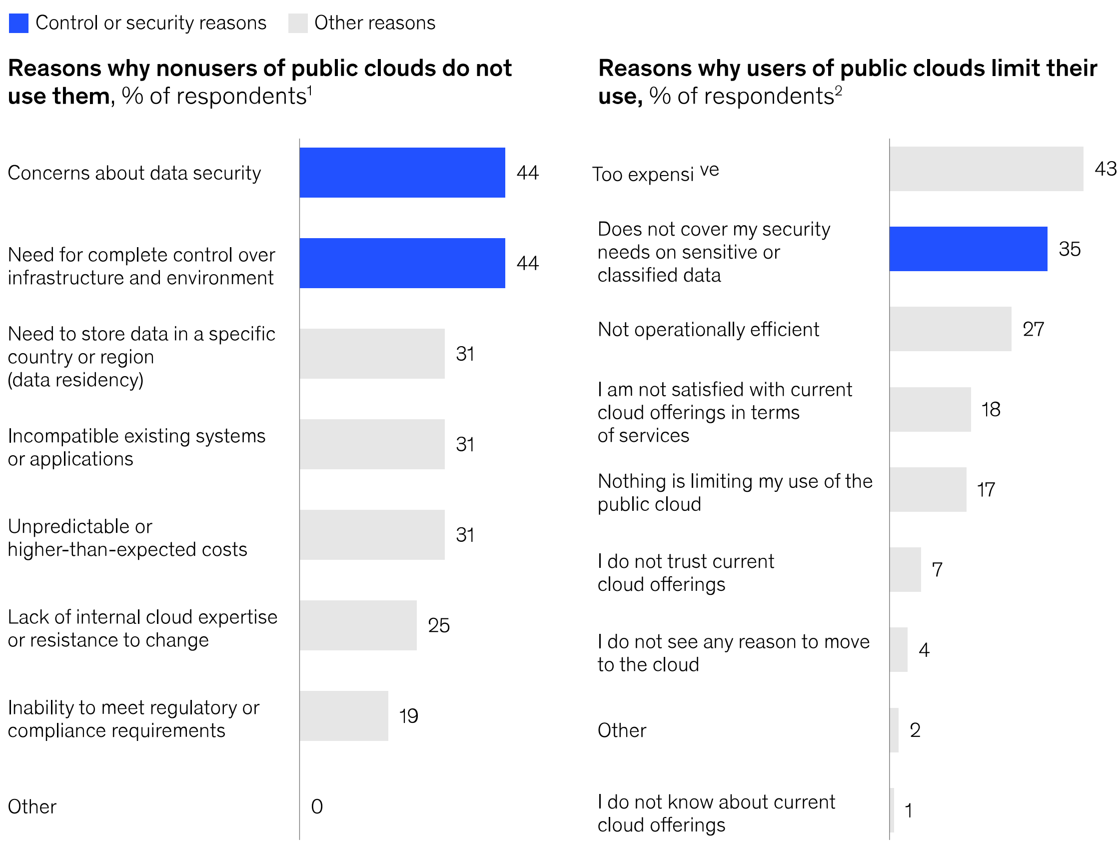
[1] In this article, we define technology sovereignty as a nation's or region's ability to develop and control critical technologies aligned to its own economic, political, and social well-being.

[2] McKinsey survey of more than 100 technology leaders (CIOs, heads of IT, heads of infrastructure, and heads of cloud) in France, Germany, Italy, and Spain working at companies across industries, with 35 percent being companies with more than $5 billion in annual revenue, July 2025.

— **Technical disruption:** Geopolitical developments, trade dynamics, and regional uncertainty can influence the continuity and availability of technology services. These factors may affect real-time system performance, data movement, and the ability to update or operate mission-critical platforms—highlighting the need for more resilient architectures.

Exhibit 1

Many technology leaders have concerns about the control and security of their companies' data in public clouds.



[1]Question: You confirmed you are not using a public cloud. What are the reasons you do not use the public cloud?
[2]Question: You mentioned using a public cloud. What is currently limiting your use of the public cloud?
Source: McKinsey survey of more than 100 technology leaders (CIOs, heads of IT, heads of infrastructure, and heads of cloud) in France, Germany, Italy, and Spain working at companies across industries, with 35% being companies with more than $5 billion in annual revenue, July 2025

McKinsey & Company

— **Intellectual property and data ownership:** Governments are increasingly asserting their rights to access data of national interest, even when hosted abroad.[3] This raises questions around how much control companies have over their intellectual property and data. The issue can be particularly challenging in cross-border scenarios involving data that are considered sensitive, including AI training data, proprietary algorithms, and customer information. Companies must navigate complex regulations in situations where one country demands access to their data while another prohibits sharing it.

— **Economic exposure:** Export controls, trade measures, and shifts in policy direction, such as proposed digital exit taxes, can result in unanticipated costs for companies. These developments may add complexity to IT budgeting, especially alongside broader cost drivers such as inflation, talent availability, and increased demand for resilient infrastructure.

— **Reputational risk:** While often secondary to regulatory or operational concerns, public perception of a company can be affected by how well it is seen to manage technology autonomy and resilience. Limited transparency or unclear governance in this area may affect trust among customers, partners, and oversight bodies.

Six strategies to balance digital autonomy with innovation

Advancing digital autonomy and resilience doesn't happen overnight, but CIOs can adopt a multilayered approach that builds on existing investments and partner relationships. They can incorporate flexibility into their planning to respond to future geopolitical changes. We have identified six strategies that can help CIOs get started.

Increase the use of open source software

An open source approach is emerging as a critical lever for CIOs because it enables greater control over the tech stack; reduces dependency on proprietary vendors; and allows technology teams to audit, fine-tune, and govern models in ways that align with enterprise risk, compliance, and data privacy requirements.[4] Open source software provides an opportunity for organizations to increase control over their code base and reduce vendor lock-in. Realizing those benefits, however, will require strong internal governance, cybersecurity capabilities, and regular engagement with open source communities.

Open source is becoming even more critical in the context of gen AI. Enterprises now face key architectural decisions not only about which models to use but also about how to orchestrate the complex agent stacks. Open source models, frameworks, and orchestration layers, such as LangChain, Haystack, Ray, and Kubernetes, provide flexibility to tailor solutions, embed governance, and maintain control over sensitive data and model behavior.

We already see this approach in practice. For example, several of the world's largest banks have adopted open-source-first strategies for their gen AI stacks to enable portable, multicloud deployments of AI agents, vector databases, gateways, and observability components.[5] These

---

[3] In the United States, through laws such as the US CLOUD Act, the government can compel companies to provide data stored abroad if it relates to US investigations. China's Cybersecurity Law and Data Security Law impose rules that require companies to store certain data locally and allow government access for national security purposes. While the European Union has strong data protection laws, such as the General Data Protection Regulation, individual member states sometimes enact additional national security laws that can require data access or limit data transfers. Russia's laws require certain data to be stored within the country and grant government agencies powers to access data for security and surveillance. In India, data protection regulations are being developed, and the government has shown interest in data localization and access for security and governance reasons.

[4] "Open source technology in the age of AI," McKinsey, April 22, 2025.

[5] Matt Ashare, "Why banks are all-in on open source," *CIO Dive*, updated April 8, 2025.

banks use open source technologies to underpin a resilient mesh infrastructure capable of hosting heterogeneous AI frameworks while meeting compliance and auditability requirements.

In another example, a state-owned European lottery and gambling company implemented an open-source-first strategy that allows it to develop new technology while retaining full control over its code and system evolution. The company was able to leverage its open source development work to build and commercialize a tech platform business to resell to other European and non-European companies. Open source also allows the organization to avoid nontransparent dependencies on third-party platforms.

Embedding open source into the tech stack requires dedicated internal expertise to manage implementation and upkeep, since the support that's typically bundled with offerings is not always robust. In fact, many enterprises fail to adopt open source at scale due to a perceived lack of support and potential security risks, even when deploying managed open source solutions.

Enhance safeguards within an existing technology ecosystem

To reduce security risks, companies can implement stronger service-level agreements with technology partners, encrypt data using locally stored keys, and configure access controls to prevent unauthorized access. They can also adopt localized offerings from global cloud providers that meet national regulatory requirements. While this method does not require many changes to an existing technology stack, it requires continued partnerships with global technology providers. Thus, it can still present legal and operational complexities. Here are two examples of the enhanced safeguards approach.

Amazon Web Services (AWS) plans to launch a new European operation in Brandenburg, Germany, by late 2025 that will deliver localized cloud services using EU-based infrastructure, operations, and personnel.[6] Data access will be restricted to EU-resident employees, and services will remain operational even if disconnected from the global AWS network.[7] Ahead of this launch, AWS already offers sovereignty features through integrated controls, dedicated local zones, and AWS Outposts, where AWS services are hosted at customers' on-premise facilities.[8]

Microsoft is expanding its localized cloud efforts with the Microsoft Cloud for Sovereignty initiative, rolling out new capabilities in the second half of 2025. The program offers policy tools, automation, and compliance guardrails tailored to regional regulations, enabling companies to build secure and compliant cloud environments across Europe.[9]

Leverage joint ventures between global and local technology providers

This approach can enhance compliance and control, but it does not fully eliminate jurisdictional risk, particularly if the services provided remain subject to external legal or commercial constraints. While this setup can help ensure short-term operational continuity, long-term sustainability could require additional planning in partnership with legal teams. To mitigate

---

[6] *AWS Security Blog*, "AWS plans to invest €7.8B into the AWS European Sovereign Cloud, set to launch by the end of 2025," blog post by Max Peterson, AWS, May 14, 2024.
[7] *AWS Security Blog*, "AWS Digital Sovereignty Pledge: Announcing a new, independent sovereign cloud in Europe," blog entry by Matt Garman and Max Peterson, AWS, October 24, 2023.
[8] "Built, operated, controlled, and secured in Europe: AWS unveils new sovereign controls and governance structure for the AWS European Sovereign Cloud," Amazon, June 3, 2025.
[9] *Microsoft on the Issues*, "Microsoft announces new European digital commitments," blog entry by Brad Smith, Microsoft, April 30, 2025.

future risks, CTOs can define risk mitigation strategies that maintain system functionality and security under evolving conditions. Here are two examples of the joint venture approach.

Orange and Capgemini, in partnership with Microsoft, launched the Bleu platform, which received the French government's "cloud de confiance" label that is awarded to European cloud services with high technical and legal compliance. Though built on Microsoft technology, Bleu is operated and majority-owned by French companies, hosted in France, and aligned with the French government's SecNumCloud framework that requires cloud service providers to meet national and international laws and ensure high levels of security.[10]

S3NS, a joint venture majority owned by Thales with Google Cloud, is combining sovereign control with hyperscale capabilities. It is a French company under French law, and its Local Controls by S3NS service is already available, offering data localization in France, encryption key control, and French and European technical support. Its infrastructure includes three data centers in the Paris region, which it will operate to meet both performance and sovereignty requirements.[11]

Adopt more services from local technology providers
To create digital autonomy and operational resilience, companies can adopt local cloud providers, network services, and software solutions. At the infrastructure level, organizations can use this approach to route specific workloads—such as data backups or regulatory reporting—to their national or regional technology providers. In Europe, the cloud market is steadily advancing, but many providers still lag behind in terms of providing value-added services. Nonetheless, for the stable workloads commonly found in transactional and operational systems, European cloud providers' offerings can meet enterprise needs.

One example of this local vendor approach is the Schwarz Group's STACKIT platform, which is specifically designed as a European cloud solution to address growing concerns around data localization and regulatory compliance. Built on OpenStack and hosted entirely within Germany and Austria, STACKIT aims to keep data under EU jurisdiction.[12]

Maintain a hybrid model in which stable workloads run on a private cloud
Many enterprises have yet to realize the full economic benefits of cloud adoption, often due to limited process maturity and insufficient application modernization. While public cloud platforms offer powerful capabilities such as elastic scalability and advanced AI services, not all applications require these features. Cloud architects often face a trade-off between leveraging full cloud capabilities and optimizing costs and control. Running stable workloads that do not require elastic scalability or advanced AI services in a private environment can provide a cost-effective regional alternative. Here are two examples of the private-cloud approach.

BNP Paribas established an extended partnership with IBM: BNP hosts IBM Cloud hardware in its own data centers, creating a dedicated on-premise IBM Cloud zone. This allows the bank to run regulated, stable workloads in a sovereign private-cloud environment while still using IBM's services, helping it comply with EU rules such as the Digital Operational Resilience Act.[13]

---

[10] "Capgemini and Orange are pleased to announce the launch of commercial activities of Bleu, their future 'cloud de confiance platform,'" Capgemini, January 15, 2024; "Capgemini and Orange announce that Bleu will start engaging with customers by the end of 2022," Orange, June 22, 2022.
[11] "Local controls with S3NS," S3NS, accessed November 3, 2025.
[12] "Companies of Schwarz Group and Google to sign partnership to jointly deliver sovereign, secure workplace productivity solutions for Germany and Europe," Schwarz Group, November 14, 2024.
[13] "BNP Paribas signs a new multi-year partnership agreement with IBM Cloud," IBM, April 29, 2025.

The European Space Agency's Ask ESA platform is a secure, on-premise gen AI platform built in cooperation with DXC Technology. It allows ESA staff to create AI agents that search and interact with internal scientific and operational data, making it a sovereign tool for nonpublic use.[14]

Design portable architectures for critical workloads

By building their own cloud-native architectures that use best-practice governance frameworks, companies can forge a path toward workload portability. This means they could rapidly shift workloads between cloud service providers or migrate to private clouds if circumstances demand. Workload portability helps organizations future-proof their technology stacks—not only reducing exposure to regulatory complexity and minimizing service disruption risks but also providing greater protection against vendor lock-in. However, it can be complicated and expensive to build portable architectures, making this solution impractical for all types of workloads. Since migrating applications between clouds is difficult, portable architectures are best used for a select subset of applications and as part of a broader compliance or business continuity strategy.

One example of this portable approach is Telefónica's Cloud RAN deployment. The company virtualized functions of its 5G radio access network (RAN)—the portion of a mobile network that connects end-user devices to the core network—using Ericsson's open architecture hosted at a large data center in Offenbach, Germany. This enabled Telefónica to decouple RAN software from its proprietary hardware, allowing it to add or remove components more rapidly, and from a variety of vendors in the future. Thus, the telco is more flexible to adapt and scale based on business needs.[15]

While the future of geopolitics remains uncertain, inaction is not an option. Proactive CIOs will approach technology sovereignty as a strategic advantage rather than a constraint. This begins with assessing regulatory risks, understanding the potential business impacts of service disruptions, and defining the minimum viable enterprise, or the core capabilities required to maintain critical operations during periods of disruption. CIOs can then take a metered approach to risk management while still capturing the rewards of digital transformation. Ultimately, digital autonomy is not about isolation but intelligent interdependence—anchoring control where it matters most while remaining open to the innovation that drives progress.

Arnaud Tournesac is a partner in McKinsey's Paris office, **Klemens Hjartar** is a senior partner in the Copenhagen office, **Matteo Martinelli** is a partner in the Milan office, and **Rossana Lo Re** is an associate partner in the London office.

This article was edited by Kristi Essick, an executive editor in the Bay Area office.

[14] "DXC helps European Space Agency launch gen AI agents," DXC, February 13, 2025.
[15] "New network architecture with a world premiere in Offenbach, Germany: o2 Telefónica deploys first Ericsson Cloud RAN in a 5G standalone network," Ericsson, March 3, 2025.