● Whitepaper

Preparing for a Cloud migration: “No regrets” action plan



eraneos

Contents

Executive summary 3

Roadmap for preparing for a cloud transition 4

Step 1: Inventory cloud applications used 5
Step 2: Conduct a risk analysis 5
Step 3: Develop a transition strategy 6
Step 4: Establish a sourcing strategy 7
Step 5: Strengthen governance 7
Other preparatory work 9

Final thoughts 10

Get in touch 11

Executive summary



Nabeel Siddiqie
Cybersecurity Partner
Eraneos

nabeel.siddiqie@eraneos.com

In today’s digital landscape, many organizations in Europe face a critical challenge: their heavy reliance on the services of US-based Cloud Service Providers (CSPs) like Microsoft, Amazon, and Google. This dependence has created a strategic vulnerability, concentrating essential IT infrastructure under a handful of distant and foreign companies. As the geopolitical and technological landscapes evolve, these dependencies bring risks that can no longer be ignored.

Recent events, such as increasing scrutiny on data sovereignty and privacy, have amplified the urgency of addressing this dependency. Policies and standards are now urging organizations to prioritize transition planning. On March 19, 2025, the Dutch House of Representatives adopted motions highlighting the political will to reduce reliance on American CSPs. Across Europe, this focus on digital sovereignty continues to grow specially within the Financial industry with country-specific data residency requirements—such as BaFin’s cloud outsourcing rules in Germany or FINMA’s circulars in Switzerland—often mandate that sensitive financial data remains within national or EU borders. The UK’s Data (Use and Access) Act 2025 updates data sovereignty by allowing more flexible data transfer rules while maintaining core protections, creating a distinct yet complementary framework to the EU’s regulations

Initiatives such as GAIA-X and the European Alliance for Industrial Data, Edge, and Cloud aim to create a secure, sovereign, and transparent cloud ecosystem for the continent’s businesses and governments.

The potential consequences of failing to address these dependencies include interrupted digital service continuity, non-compliance with legal standards, and stifled autonomy in strategic decisions. While a wholesale departure from US CSPs is unlikely in many cases, given the lack of comparable alternatives, it remains important to have a plan in place for unforeseen developments, including changes in policy or technology that could restrict American CSPs usage. Organizations in the public and private sectors must carefully evaluate their ability to independently execute cloud transitions and assess the risks posed by inaction.

The good news is that proactive preparation also offers opportunities: it allows organizations to reevaluate their current cloud strategies and create a future-proof system that aligns with their goals, business continuity, and security requirements. This whitepaper provides a six-step framework to help organizations prepare for any eventualities in cloud transition – ensuring digital resilience without regrets.

Roadmap for preparing for a cloud transition

Involving external specialists can offer valuable insights, reduce likelihood of mistakes, and accelerate the process.



Delaying action until there is an urgent need for a cloud transition, such as a CSP unexpectedly terminating its services, significantly increases the risk of disruptions to critical business processes. To prevent such a scenario, it is essential for organizations to take proactive steps that enhance their resilience. These actions, referred to as “no regrets” measures, provide immediate value by clarifying dependencies and reducing risks, even if a migration is not currently planned.

Organizations with sufficient internal expertise and resources can implement these measures independently. However, involving external specialists can offer valuable insights, reduce the likelihood of mistakes, and accelerate the process. Professional support can act as a key advantage. At Eraneos, we are prepared to help organizations navigate this journey, leveraging experience to provide strategic and actionable advice.

The most important takeaway is to begin immediately. By acting now and following the steps outlined below, organizations can ensure they are prepared for a smooth transition whenever it becomes desirable or necessary to move away from a US-based CSP. This roadmap consists of five structured steps, developed in alignment with recognized best practices and compliance standards. These steps can be approached in parallel to maximize efficiency. Where relevant, references to existing industry frameworks and standards are included to ensure a methodical and compliant process.

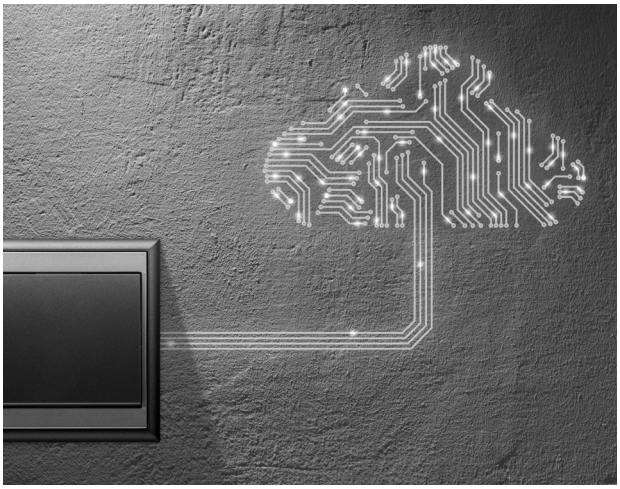
Step 1: Inventory cloud applications used

Preparing effectively for a potential cloud migration requires a clear understanding of what is running in the cloud and the possible impact of service disruptions. The first step in this process is conducting a comprehensive inventory of all cloud applications, services, and underlying infrastructure. For each cloud application, organizations should gather key details such as the type of data stored, the functionalities provided, and the integrations with other systems.

The inventory should cover both technical components, such as virtual machines, databases, and functions, as well as the business processes they support. This involves identifying which business operations rely on cloud applications and determining which of these processes are critical. These insights will inform migration priorities and the order in which systems need to be addressed. Assets should also be assessed for sensitivity and criticality by asking questions such as: which data is confidential or privacy-sensitive? Which applications are essential to business continuity, and which can withstand short periods of downtime?

To streamline and modernize the inventory process, automated tools can be utilized. Solutions like Cloud Management Platforms (CMPs), asset discovery tools, or “infraestructure-as-a-code“ platforms can make data collection more efficient and accurate. Examples include Azure Migrate, AWS Application Discovery Service, and integrations with ServiceNow’s CMDB. These tools are invaluable for mapping dependencies, visualizing network topology, and understanding data flows. These insights are critical when planning an exit or migration.

In summary, completing this step results in a current and detailed cloud asset registry. This includes an inventory of data and its classification, forming a strong foundation for comprehensive transition planning.



Step 2: Conduct a risk analysis

Effective preparation demands a thorough understanding of potential risks. The second step involves identifying and assessing scenarios and their associated risks related to a forced or planned cloud transition. Examples of such scenarios include large-scale privacy breaches, significant price increases, service outages at the provider, or government policy changes that restrict the use of US-based cloud providers. For each scenario, it is essential to evaluate the potential impact on the organization and the likelihood of the scenario occurring for every cloud application. This assessment helps to rank risks by severity to determine which require higher priority.

A key aspect of the risk analysis is evaluating the risk of vendor lock-in. This involves analyzing how the availability of data and services could be affected when switching to a new environment. Additionally, considerations should include how quickly a migration could be executed, what dependencies exist, and which business processes or external stakeholders might be impacted. By addressing these elements, various exit scenarios such as an immediate cessation versus a phased transition can be developed, and the residual risks for each scenario can be identified.

Beyond assessing risks, it is advisable to estimate the potential costs of an exit, referred to as the Total Cost of Exit (TCoE). These costs could include data migration, modifications to licenses, temporary duplication of infrastructure, and the staffing required for the transition. By estimating these costs in advance, organizations can build realistic scenarios and avoid unexpected financial challenges during implementation. This also helps to establish a stronger business case for proactive preparation.

The output of this step is a clear understanding of the risks associated with a cloud transition as well as an overview of anticipated costs. This insight forms a foundation for making informed decisions and strengthens the organization‘s readiness to manage transitions effectively.



Cloud applications are diverse and require their own approach. Some services are easy to transfer, while others require major adjustments.

Step 3: Develop a transition strategy

With a clear understanding of the cloud landscape (Step 1) and the risks associated with each application (Step 2), the organization can focus on creating a practical approach to handle a cloud transition. This step involves developing a detailed strategy for exiting a cloud application, whether the exit is gradual or occurs due to an emergency. At the same time, it is essential to consider alternatives, such as potential migration destinations and how to avoid becoming locked into a specific provider again. This can be formalized as part of the sourcing strategy.

Cloud applications vary significantly and require tailored approaches. While some services are straightforward to transfer, others may demand significant modifications. It is, therefore, prudent to define migration paths in advance, such as whether to move, adapt, replace, or divest specific applications or services. Additionally, dependencies must be thoroughly considered. Questions to address include which APIs, data exchanges, or integrated services need to be included and how critical business processes will be safeguarded against interruptions. A phased migration approach, prioritizing the least complex systems first, can help in spreading and mitigating risks.

It is also recommended to regularly rehearse and refine these plans. For example, organizations could practice by annually migrating a subset of applications and data to a secondary environment and then back again. More intricate strategies can be evaluated through tabletop exercises. These exercises help identify gaps, provide insights into recovery times, and highlight areas for improvement. All findings should be documented, and the transition strategy updated accordingly.

By the end of this step, the organization will have a well-defined plan for phasing out cloud applications. This plan will include clearly outlined recovery procedures and migration paths, ensuring readiness for any cloud transition scenario.

Step 4: Establish a sourcing strategy

In conjunction with preparing for a possible transition, it is vital to plan for future sourcing. Organizations should identify potential alternatives that may be leveraged after a cloud transition and address how to avoid renewed vendor lock-in.

To minimize lock-in and improve flexibility, organizations can implement a multi-cloud or dual-vendor strategy. This approach involves distributing services across multiple CSPs, with special attention given to ensuring data and workload portability. Developing a sourcing portfolio is also beneficial, as it enables ongoing evaluation of CSPs using key criteria such as cost, compliance, data sovereignty, and technological innovation. This structured method allows for well-informed sourcing decisions that align with both current and future organizational needs.

A cloud transition does not necessarily mean exiting the cloud entirely. In some cases, it may involve transitioning to a different provider, like a European CSP that offers stronger assurances around sovereignty and compliance. When selecting a new CSP, organizations must carefully evaluate critical factors such as legal and compliance requirements, technical capabilities, costs, and long-term scalability.

At the conclusion of this step, the organization will have a clear understanding not only of how to exit their current cloud environment but also of where to migrate if required. This ensures that the organization remains in control of its strategic and operational priorities throughout the transition process.

Step 5: Strengthen governance

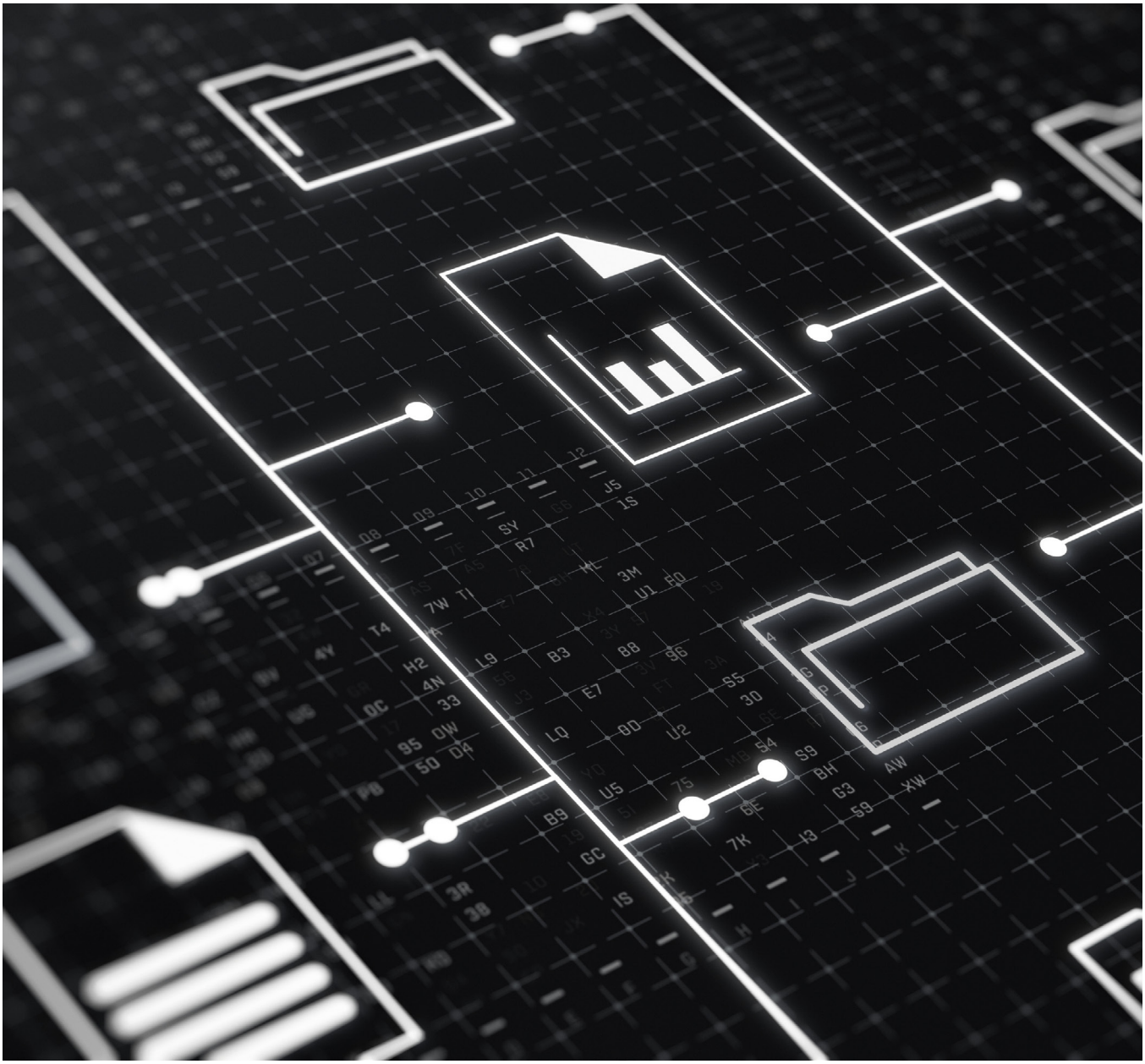
Strengthening governance is a vital step to embed transition and sourcing strategies into the organization‘s operational and strategic framework. These strategies should not be treated as one-off documents but as living components of the governance cycle, ensuring continuous alignment with policies, processes, and controls. This proactive approach is key to maintaining long-term resilience and adaptability.

Policy and governance integration
Transition preparedness should be incorporated into existing policies and architecture governance. For every cloud application, organizations should evaluate how it could be replaced if necessary. This ensures that exit plans are developed for all current and new cloud solutions. Regulations such as the **BIO standards framework and the Digital Operations and Resilience Act (DORA)** emphasize the necessity of exit strategies as part of business continuity management, elevating this practice to a managerial priority.

Procurement and business unit involvement
Procurement plays a pivotal role in governance by securing robust exit agreements in contracts. These agreements should include clauses on exit triggers, notice periods, and vendor support for data migration. Emphasis must also be placed on sovereignty and flexibility in procurement terms. Active involvement from business units is crucial; they are best positioned to assess the impact of cloud transitions on business processes and prioritize applications based on their criticality.

Continuous evaluation through lifecycle management
Governance frameworks must consider transition readiness as part of overall **sourcing lifecycle management**. Contract renewals, supplier evaluations, and procurement processes should include structural reviews of a service’s transition potential. A maturity model can be employed to periodically assess how well cloud environments meet transition-readiness standards. This systematic approach ensures continuous improvement and prevents recurring dependencies.

Awareness and training
Awareness within the organization is essential to ensure all stakeholders are aligned. Policymakers and executives must understand the strategic significance of an exit strategy, while operational teams must be equipped to handle transitions and manage new CSP sourcing. Regular training sessions, workshops, and table-top exercises help prepare staff for both planned and emergency exits. These exercises identify gaps, enhance recovery readiness, and reinforce a culture of adaptability.



Cloud-neutral architectures: organizations can implement a design and development approach where systems and applications are not dependent on specific CSPs.

Digital resilience and strategic supplier management
Integrating transition and sourcing strategies into governance strengthens overall digital resilience. A solid exit strategy not only ensures compliance with frameworks like **ISO/IEC 27001** but also enhances supplier management. This leads to better decision-making for future cloud strategies, allowing organizations to remain flexible and in control in dynamic digital environments.

By adopting this comprehensive governance approach, organizations can ensure their cloud strategies are future-proof, highly responsive, and compliant with key standards. This proactive effort enhances preparedness, reduces risks, and positions the organization for long-term success in the evolving cloud landscape.

Other preparatory work

Contractual assurance
It is essential to analyze existing contracts with cloud service providers (CSPs) to confirm they include robust offboarding provisions. While most cloud contracts emphasize onboarding and operational services, provisions for termination are equally critical. Contracts should include explicit exit strategies, detailing:

- Exit triggers
- Notice periods
- Migration timelines
- Vendor support for data portability

If these components are missing, organizations should pursue renegotiation or add supplemental clauses during contract renewals. Moving forward, new contracts should standardize exit terms, incorporating them into procurement policies. These measures reduce ambiguity, streamline potential migrations, and lower operational disruption risks during a transition.

Backups Outside the Cloud
To reduce the risk of vendor lock-in, organizations should maintain regular backups outside the cloud, such as on-premises or in secondary environments. These backups must be formatted for portability, enabling them to be readily used for recovery during an exit scenario. This ensures that critical data remains accessible and operational independence is preserved.

Cloud-neutral architectures
Cloud-neutral architectures prioritize flexibility by designing systems and applications that are not dependent on a single CSP. Implementing these principles allows organizations to:

- Migrate between CSPs without significant reconfiguration
- Transition to hybrid environments
- Return to on-premises infrastructure if necessary

This approach fosters adaptability and sustains long-term independence in a dynamic cloud ecosystem.

Escrow as a last resort
Source code escrow arrangements provide a safety buffer in the event of a sudden CSP failure. These agreements ensure that source code remains accessible even if the provider ceases operations. Regular reviews of escrow terms for timeliness, completeness, and usability are critical. For key SaaS services lacking escrow provisions, alternatives – such as monthly data exports to a trusted third party (e.g., a notary) – should be considered. This prevents a scenario in which an organization loses access to its critical resources.

Fallback environment
Establishing a fallback environment ensures that the organization can continue to operate during CSP outages. Options range from minimal on-premises infrastructure for critical services to predefined infrastructure-as-code (IaC) scripts that allow rapid deployment to an alternative cloud platform. While full redundancy may not be cost-effective, organizations must at least define how quickly operations can be restored in such scenarios. Regular practical tests are essential to refine response times and validate fallback readiness.

Legal control
Contracts with CSP’s should explicitly address data residency and legal control over organizational data. For example, stipulating that all data be stored and processed within the EU can reduce exposure to foreign jurisdictions, such as the U.S. CLOUD Act. For industries with stringent regulatory requirements (e.g., healthcare, government, financial services), this is a critical focus area during contract negotiations and risk management planning.

Benefits of these preparatory measures
These actions create a safety net, ensuring that the organization can continue to function even if access to a US CSP is abruptly terminated. While the organization may need to scale back temporarily in such scenarios, essential operations and data integrity will be preserved.

Additionally, these measures strengthen the organization‘s negotiation position with CSP’s. By demonstrating the ability to exit a provider‘s services smoothly, the organization incentivizes higher-quality service and transparency from its CSP partners in regular operations. This results in better operational outcomes and aligns the organization‘s cloud strategy with its long-term goals for resilience and flexibility.

Contact:



Nabeel Siddiqie
Cybersecurity Partner
Eraneos

nabeel.siddiqie@eraneos.com



Julian Meyrick
Cybersecurity Partner and UK lead
Eraneos

julian.meyrick@eraneos.com



Ralph Erhard
Financial Services Global Lead - Partner
Eraneos

ralph.erhard@eraneos.com



Carlo Gebhardt
Cybersecurity Global Lead - Partner
Eraneos

carlo.gebhardt@eraneos.com

Final thoughts

By taking the steps above, organizations are building a solid foundation for any transition from US cloud environments. This roadmap focuses on “no regrets” actions. These steps deliver immediate value in the form of better insight, reduced dependency, and higher compliance, regardless of whether migration ultimately occurs or not. In essence, organizations are insuring themselves against future uncertainty in the cloud landscape.

The urgency to take action is clear, with growing concerns about vendor lock-in, data sovereignty, and explicit requirements from policies and standards to have transition planning in place. Fortunately, the approach is practical and achievable. Many of these steps align with normal IT governance and security practices that are already part of existing policies and best practices.

Transition preparation also provides an opportunity to reassess broader sourcing issues. Does the current cloud strategy still fit the organization‘s ambitions? Are there better combinations available using public, private, or hybrid models? By linking transition planning to sourcing and architecture policies, organizations can create a future-proof and agile cloud approach. With this strategy, policymakers, IT managers, and CISOs can begin strengthening their organization‘s digital autonomy and resilience. While much of the preliminary work can be done internally, engaging specialists, where needed, is a sensible investment to accelerate progress, particularly for automating asset inventories or implementing cloud-neutral architectures.

This is ultimately a call to action: prepare for a transition now. By acting today, organizations will keep all options open in the future and reduce risk and costs in an ever-evolving cloud environment. Even if migration never becomes necessary, proactive preparation generates lasting value in the form of better cloud decisions, stronger contracts, and greater control in vendor relationships. This ensures organizations remain in control, regardless of changes in the cloud landscape.

Be prepared for a transition, even if you hope it will never be needed. Eraneos is ready to guide organizations through this journey.



Get in touch

Nabeel Siddiqie
Cybersecurity Partner
Eraneos
nabeel.siddiqie@eraneos.com

Julian Meyrick
Cybersecurity Partner and UK lead
Eraneos
julian.meyrick@eraneos.com

Ralph Erhard
Financial Services Global Lead - Partner
ralph.erhard@eraneos.com

Carlo Gebhardt
Cybersecurity Global Lead - Partner
carlo.gebhardt@eraneos.com