Deloitte.

Sponsored by aws

Powering Europe's Digital Edge

Cloud Adoption in Europe's Critical Industries

Table of Content

Demographics and Methodology

This report, commissioned by **AWS** and conducted by **Deloitte**, explores the role of cloud in driving digital transformation and competitiveness across critical industries in Europe. The study focuses on identifying success stories of European cloud customers and how they use state-of-the-art cloud technologies to securely scale, innovate, and compete globally.

Data for this report was collected through an approach that combined in-depth interviews with a detailed questionnaire and desk research conducted between February 2025 and August 2025. The aim was to capture qualitative insights based on discussions with professionals involved in decision-making on aspects related to cloud strategy for large European companies in critical sectors and public sector organisations. The profile of the respondents included CIOs, CTOs, heads of infrastructure, infrastructure architects and IT Directors.

The study includes inputs from 33 large organisations from across 14 EU Member States, operating across critical sectors such as finance, health and life sciences, telecoms and media, energy, public sector and defence, a majority of which exceed EUR 1billion in annual revenue.

The findings presented in this report are based on the insights and data collected and do not represent the opinions or views of Deloitte.

Figure 1 - Respondents Yearly Revenue and Industry

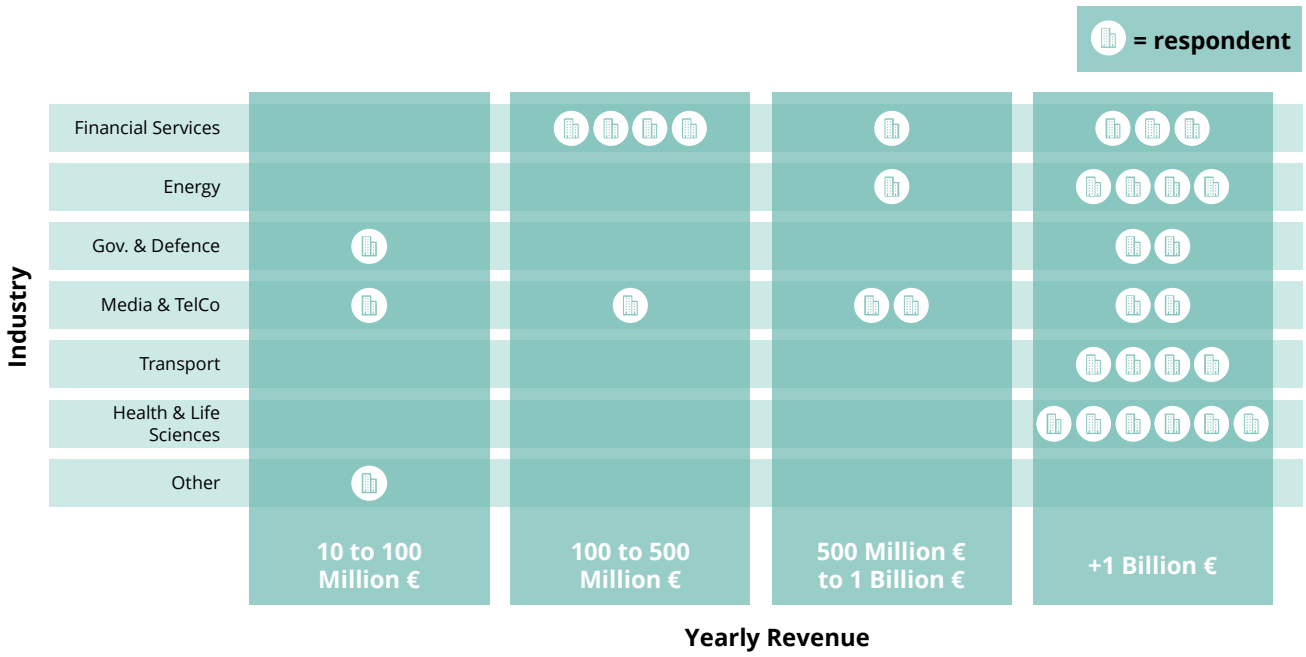
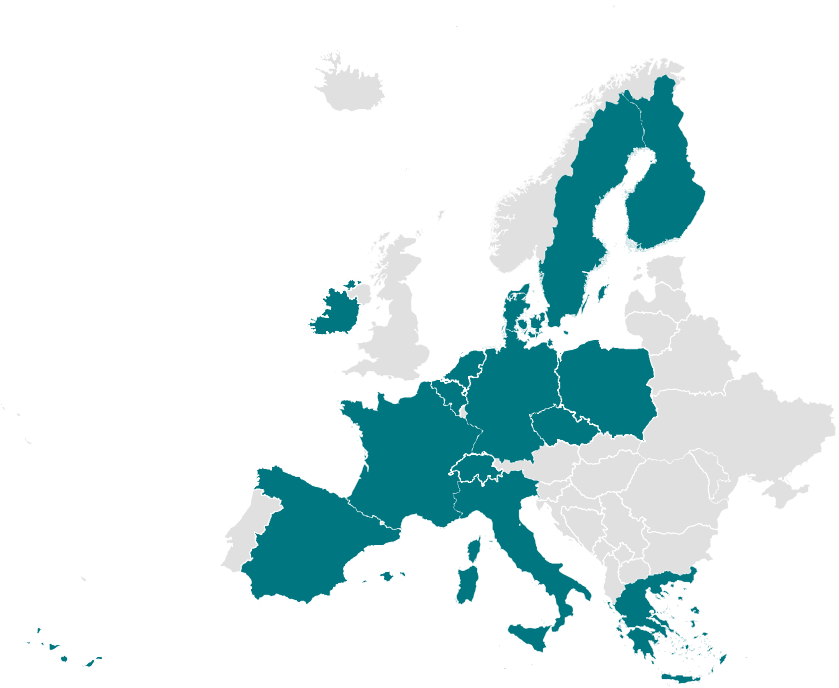


Figure 2 - Geographic Region

- Belgium
- Czech Republic
- Germany
- Sweden
- Poland
- Spain
- Finland
- Netherlands
- France
- Denmark
- Italy
- Ireland
- Greece
- Switzerland



Motivations for Cloud Adoption and its Benefits

In today's dynamic digital landscape, companies are increasingly adopting cloud computing, viewing it not merely as a technological upgrade but as a fundamental shift that significantly expands their capabilities. Companies are also moving quickly by scaling their operations, accelerating their time-to-market for new products, and the cloud's evolution aligns with this pace.

However, when looking at cloud expenditure, the study finds that a majority of participants **dedicate less than 10% of their IT budget to cloud infrastructure (see chapter on cloud expenditure, p.19)**. These figures fall below industry benchmarks for hosting, suggesting that a substantial volume of workloads remains within on-premises infrastructure[1]. This aligns with data available at global level, where less than 15% of IT spend is on cloud services and approximately 70% of IT workloads are on-premises[2].

In 2019, bpost faced a choice: invest in new hardware and data centre capacity or move to the cloud for its hosting environment. They decided to move to the cloud because it offered a path to better overall security and perfectly aligned with their growing parcel business. They anticipate significant seasonality at the end of the year when volumes will double or triple. In a classic on-premises setup, they would have to invest in permanent capacity for that peak. The cloud, however, allows them to easily adjust resources to match demand at any given moment.

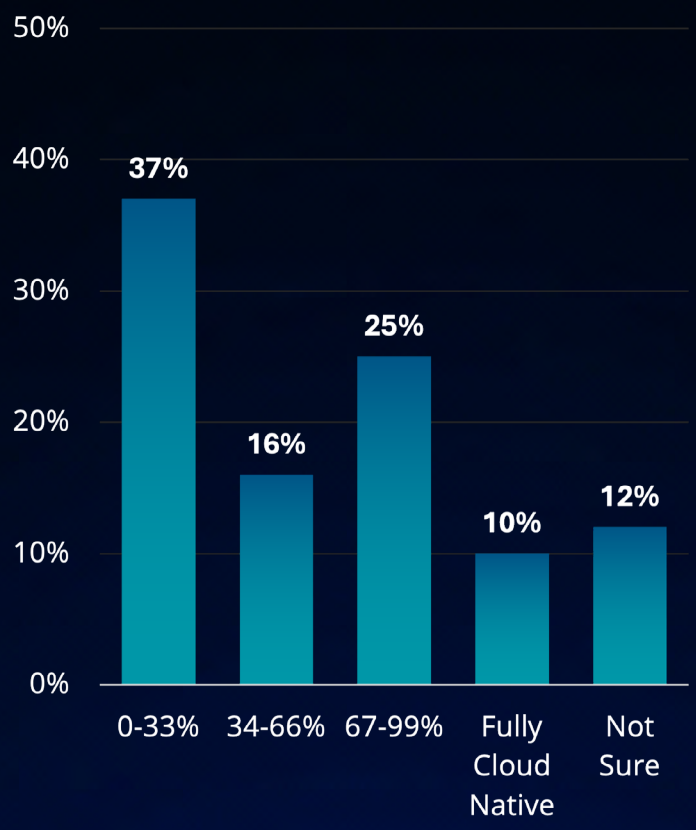
> We were very lucky with our timing because when COVID hit, it caused a huge, sudden surge in demand for system capacity. We were able to handle it thanks to the flexibility of the cloud. Otherwise, we never would have been able to cope with the unpredictable situation. Now, it's far easier and more flexible to experiment with new technologies like AI, data insights, and machine learning.
>
> **- Bart Van Dorpe, CIO, bpost**

[1] IT Key Metrics Data 2026: Industry Measures — Executive Summary
[2] https://www.goldmansachs.com/insights/articles/cloud-revenues-poised-to-reach-2-trillion-by-2030-amid-ai-rollout

In line with these findings, only **10% of participants are fully cloud native**, meaning they have 100% of their workloads running on the cloud, while others are in different phases **of migrating existing workloads**. This group breaks down into three distinct phases of progress: 37% are in the early stage, having migrated 0–33% of their workloads; 16% are in the mid-stage, with 34–66% migrated; and 25% are in the late stage, having completed 67–99% of their migration projects.

> The cloud has truly become the new normal for operations. Everything is in the cloud; it provides a catalogue of services and an environment that is so much easier to deal with compared to on-premises.
>
> **- Olivier Philippe Convard, VP and Head of Product Security and Privacy Organization, Roche Diagnostics**

Figure 3 - Percentage of total workloads migrated to cloud



While early cloud adoption was primarily driven by direct infrastructure cost reduction, the move to cloud is now motivated by a broader range of advantages. These include agility, innovation, overall cost optimisation, and enhanced infrastructure, such as improved resilience, global reach, and stronger security compared with on-premises. These benefits collectively contribute to a more agile, resilient, and competitive business framework, essential for success in the current business environment.

The most significant driver for cloud adoption is the **enhancement of speed, agility, scalability and flexibility in product development and operations**, cited by 82% of the participants. This enables organisations to adapt to market changes efficiently, maintaining a competitive edge. The second most important driver, mentioned by 64% of respondents, is **access to innovation**. The cloud allows companies to easily utilize cutting-edge technologies like AI, machine learning, and big data analytics to drive continuous improvement and growth. **Improved security, data protection, and regulatory compliance** with cloud are the third most prioritized driver of adoption for 48% of participants. The robust security measures offered by the cloud help organizations safeguard sensitive information and adhere to stringent regulations, providing peace of mind and mitigating risk.

Figure 4 – Companies planning to expand their cloud footprint by migrating on-premises or private cloud workloads to the public cloud

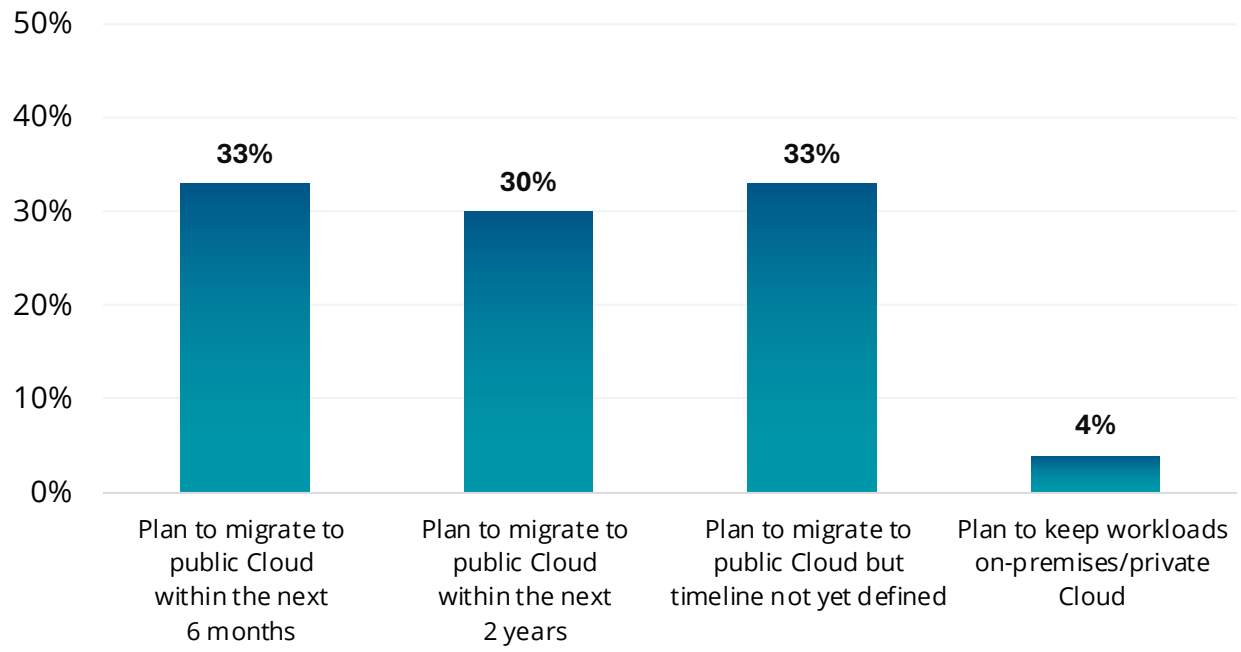


Figure 5 - Cloud adoption drivers

When COVID hit, every shop went online, and our business experienced massive growth. We knew immediately that ordering physical servers and setting them up in our own data centres just wouldn't work; we'd never keep up. The ability to instantly scale with cloud has been critical. It allows us to seamlessly handle huge spikes for events like Black Friday or Cyber Monday, something that would be impossible and prohibitively expensive if we tried to manage it ourselves.

- Cian O'Driscoll, Head of Engineering and Europe CIO, Stripe Technology Europe

European Companies Use Cloud to Increase Speed, Agility, Scalability and Flexibility in Product Development and Operations

Among the shared benefits of cloud computing, increased scalability and flexibility were highlighted by 82% of the participants. Participants gain the ability to rapidly implement and scale cloud resources (such as virtual machines, storage, and databases) to meet fluctuating demands, all without the constraints of on-premises investments. This elasticity ensures resources are consistently optimized, preventing both under-provisioning (which can lead to performance bottlenecks) and costly over-provisioning (resulting in wasted expenditure). Such on-demand scaling has been identified as crucial by most participants; the challenges posed by COVID-19 served as a clear example of the cloud's role in supporting business agility during uncertain times. This allowed participants to scale in accordance with spiking demand without having to manage and run data centres.

This agility also translates into a much faster product lifecycle. While the breadth of cloud services naturally streamlines development and time-to-market, a key finding of this study is the value participants place on how cloud enables a product-centric operating model, combined with adopting an innovation mindset. The cloud's inherent flexibility and on-demand resources significantly lower the cost and risk associated with experimentation, allowing teams to rapidly prototype, test, and quickly identify what works and what doesn't. This "fail-fast" approach means that potential issues or unviable ideas are discovered early, minimising wasted effort and accelerating successful solutions.

The cloud also provides the frameworks and capabilities to efficiently structure and manage products at scale. It enables the organisation of self-sufficient teams with autonomy, while simultaneously offering guidelines and guardrails for secure and responsible cloud service usage. Beyond this, cloud services, with their integrated DevOps, enhanced security, and modern development tools, are now central to driving innovation and operational excellence, allowing participants to iterate and improve at a rapid pace.

> We started our cloud journey a decade ago and are now using cloud services across our entire business. The main motivations ultimately come down to scale, efficiency, and resiliency - capabilities that we are actively building out, and, for which, leaning into the cloud is critical.

-Dimitrije Jankovic, Global Head of Digital Strategy and Operations, Sanofi

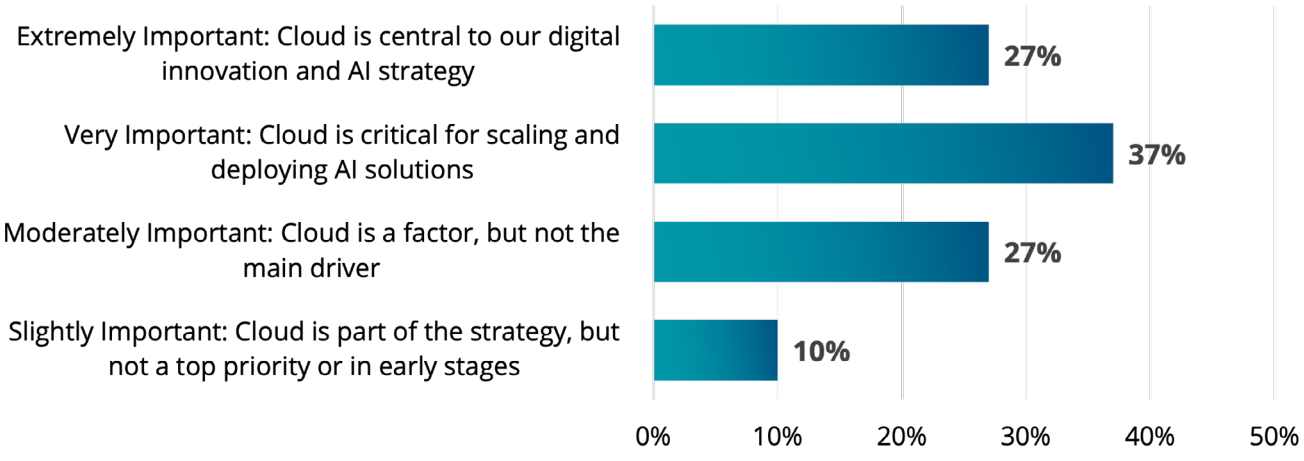
Sanofi aspires to be an R&D-driven, AI-powered biopharma company. It understands that to make AI effective, it needs a foundation of high-quality data. This data is generated by reliable applications and processes, which are often hosted in the cloud. Recognizing the cloud's crucial role in AI-powered analysis, Sanofi has built a robust multi-cloud environment to fully leverage these capabilities.

Innovation is the Second Most Important Factor for European Companies when Choosing Cloud Services

Thanks to the reduced need for extensive foundational technology development on the cloud, participants are empowered to consume and experiment with more advanced technologies. This allows for the testing of new technologies with significantly lower effort compared to on-premises environments. The immediate availability of cutting-edge cloud services (e.g., AI/ML, IoT, analytics) provides ready-to-use tools and platforms that accelerate innovation.

Using the cloud for innovation can serve as a critical competitive advantage, particularly in highly competitive markets, as demonstrated by the experiences of agile fintech companies. A point shared among 64% of participants, who view the cloud as very or extremely important for scaling and deploying AI solutions. This sentiment is even stronger among participants with a global footprint, where 83% share this view. This data underscores that for European companies seeking to boost their competitiveness in global markets and establish market leadership, having access to cloud technologies is viewed as essential.

Figure 6 - Importance of cloud adoption in digital innovation and AI adoption strategy of European companies



By offloading the complexities of infrastructure management to cloud providers, participants can reallocate internal IT resources and talent to focus more intensely on core business activities and strategic innovation. However, it's crucial to understand that this doesn't eliminate the need for people to manage the cloud. Instead, the focus shifts from hands-on infrastructure maintenance to higher-level cloud management tasks. Skilled individuals remain instrumental to oversee cloud configurations, optimise costs, manage security, and ensure compliance. They also play a central role for setting up and maintaining cloud-wide automation to use cloud services to their full potential. This enables teams to move beyond day-to-day operational burdens and truly drive innovation. We expect AI to further empower customers to manage their cloud usage and reduce costs by automating technical and governance tasks, thereby closing the gap created by the lack of specialized skills.

> To remain competitive, it is essential to understand cloud capabilities and available choices. Cloud lowers entry barriers for proof of concepts and promotes hands-on learning, which is simply not feasible on premises.
>
> **- Krzysztof Jeger, IT Service Director, Volkswagen Group Polska**

> Innovation and cloud go hand in hand, you can't have one without the other.
>
> **- VP, Datacentre Infrastructure of a market-leading telecoms provider in a major European country with multi-billion-euro revenue**

> We train our AI models using powerful public cloud resources, with the data stored in our on-premises data centres. Once trained, we bring the models back in-house and run them on-premises for more operational side of things.
>
> **- Director of cloud infrastructure of a multinational pharmaceutical company employing tens of thousands of people**

> The main driver for cloud adoption in healthcare is the need for AI, which requires immense computing power for algorithm development, research, and analysis of results. This cannot be done in-house. For sharing information, storing data, and performing all the analyses on real-world patient data, you need serious computing power just to get results quickly. I truly believe cloud is the accelerator.
>
> **- Senior representative of a multinational healthcare company with annual revenues in the tens of billions of euros**

European Companies Choose Cloud for Increased Security, Resilience, Data Protection and Regulatory Compliance

Cloud environments offer infrastructure that fundamentally enhances security and resilience. The increasing importance of data protection, cybersecurity and resilience obligations has made cloud adoption a strategic move, directly supporting compliance efforts. **48% of participants have highlighted that a key advantage of cloud providers regarding security** is that they can invest far more time, money, and effort than individual participants can to manage on-premises infrastructure. This dedication directly translates into a better security for participants.

Cloud providers further simplify security compliance with a vast array of global, European, national, and industry-specific standards (e.g., SOC 2, ISO 27001, GDPR, DORA, NIS2, HDS, C5, ENS, Italian cybersecurity accreditation for the public sector, EBA Outsourcing guidelines, etc.). cloud providers embed security best practices into their services and offer tools to help customers implement these, from identity and access management to data encryption. Crucially, participants using the cloud benefit from cutting-edge security infrastructure without needing to make substantial capital and operational investments.

> We consistently face sophisticated security threats targeting banks. Cloud technology gives us a clear advantage, offering better data protection and distribution across multiple regions, which simplifies replication across multiple data centres. Innovation is another key benefit; we can immediately leverage the latest security features released by our providers. The Cloud business, much like banking, is built on trust, and a strong track record of security is non-negotiable for our cloud service providers.
>
> **- CTO of a large retail and wealth management bank in the Nordics with AUM in billions of euros**

> Leveraging the Cloud has undeniably improved our security. This isn't just about problem prevention; it's also about resiliency, redundancy, and recovery time. Whether it's prevention or managing an incident, the Cloud ensures we can recover far more quickly.
>
> **- Rafael Blesa Martinez, CIO, Naturgy**

> There is an analogy - If you want to save money, do you save it under the mattress, or do you put it in the bank? Moving from an on-premises to a Cloud infrastructure is similar. Cloud ensures security, unlocks scalability, optimization, and experimentation with a lower upfront cost.
>
> **- Olivier Philippe Convard, VP and Head of Product Security and Privacy Organization, Roche Diagnostics**

Cloud environments also offer robust capabilities for disaster recovery. By distributing data and applications across multiple redundant servers and geographically dispersed data centres, cloud providers offer high availability and resilience against outages or catastrophic events. This built-in redundancy and automated failover mechanisms of selected services significantly simplify the implementation of comprehensive disaster recovery strategies. For some participants, this capability was a decisive factor in their cloud adoption journey; one notable instance involved a company that experienced a significant incident in its on-premises data centre, prompting its move to the cloud to achieve greater resilience and improved operations. Multiple participants specifically highlighted that the cloud's ability to facilitate rapid global expansion was a key driver, effectively leading to "one less thing to think about" when expanding their business.

While cloud providers offer robust security for the underlying infrastructure, customers are responsible for securely configuring the services they use and data they put in the cloud. Several participants highlighted the challenge of effectively securing these cloud environments, noting it requires specific knowledge.

Cost Savings are still One of the Top Factors for Companies to Choose Cloud

About 40% of participants place the financial and operational advantages of the Cloud on the 4th place of driver for adoption. Financially, the Cloud eliminates the need for massive upfront hardware investments (capital expenditure), shifting to a flexible pay-as-you-go model (operating expenditure) that helps businesses save money and avoid paying for idle capacity. Operationally, it allows companies to offload the complex task of running data centres, freeing up IT teams to focus on core business tasks and enabling them to easily scale resources up or down to meet fluctuating demand.

Cloud computing was once seen in past reports[3] as mainly a means to reduce costs, particularly for organisations expecting significant investments to maintain or replace ageing on-premises infrastructure. However, our findings show a more complex picture.

> We've found the Cloud to be highly cost-effective. We can make decisions and immediately see the impact on our bill. In our experience, the total cost of ownership in the Cloud is significantly less than with an on-premises approach

- Rafael Blesa Martinez, CIO, Naturgy

According to Naturgy, with an on-premises setup, growth was slow and inflexible due to the long acquisition time for new infrastructure. However, The Cloud offers higher flexibility, resilience, and efficiency, along with immediate access to innovation. The quality and design of the services it gets from the Cloud would be challenging to achieve on its own. Cloud providers' numerous replicated infrastructures give Naturgy the industrial quality of service, resilience, and security that they require.

[3] Deloitte - Report on Hyperscalers Cloud Monitor in Belgium, 2023

> Cost management on the Cloud platform is a continuous effort. We actively run initiatives like hackathons to identify cost-saving opportunities, such as deleting duplicate data or scaling down servers. These efforts have significantly optimized our operational expenditure. It's crucial to constantly monitor Cloud spending, as costs can escalate quickly if you're not careful.
>
> **- Cian O'Driscoll, Head of Engineering and Europe CIO, Stripe Technology Europe**

> Cloud isn't about cost saving; it's purely about flexibility and innovation. If cost saving were the sole objective, Cloud wouldn't be the right choice.
>
> **- Bart Van Dorpe, CIO, bpost**

18% of the participants cited infrastructure cost reduction as their primary reason for moving to the cloud, while **70% of the participants believe the true advantage of cloud adoption lies in overall cost optimisation**. While 30% of the participants have experienced higher overall expenses in the cloud, these costs are often justified by the added value, such as the ability to handle more workloads, expand usage beyond previous limitations, drive innovation and accelerate time-to-market. These benefits ultimately contribute to increased business revenue.

For smaller workloads, some participants achieve lower costs by utilising Cloud-native services with a pay-as-you-go pricing model, while for large workloads, achieving cost optimisation in the Cloud demands a deeper level of expertise. Simple "lift and shift" migrations of legacy applications are often suboptimal because they don't fully leverage the Cloud's benefits. To unlock true Cloud efficiencies, these applications require refactoring, a process that demands specialized knowledge. It is expected that emerging AI capabilities will increasingly streamline and accelerate this process.

Effectively managing Cloud costs also requires robust FinOps (Financial Operations) practices and continuous usage monitoring. These initiatives, which encompass real-time consumption tracking, resource tagging, and setting budget alerts, are crucial for controlling costs and ensuring predictability.

While many participants view creating a strong FinOps culture, cost transparency, and predictability as key concerns, several of them express having already improved and standardized these practices. AI-powered solutions are likely to make sophisticated FinOps practices more achievable and efficient and help bridge the traditional gap created by the scarcity of professionals who combine both technical and business proficiency.

Additionally, implementing strong cloud governance models is essential for navigating the cloud's complexity, ensuring compliance, and controlling costs without stifling flexibility. Having the right scaling strategy to up- and downscale workloads based on consumption patterns is also a crucial element for cost control.

> As part of our digital transformation strategy, we modernised our legacy applications to microservices and containers. This enabled a safer and more cost-effective Cloud migration compared to a basic "lift-and-shift" approach. It quickly became clear that this Cloud strategy was far more cost-effective than staying on-premises, and our focus on cost optimisation and FinOps allowed us to lower expenses even further.
>
> **- Danilo Gismondi, IT Director and Digital Transformation Officer, Autostrade per l'Italia**

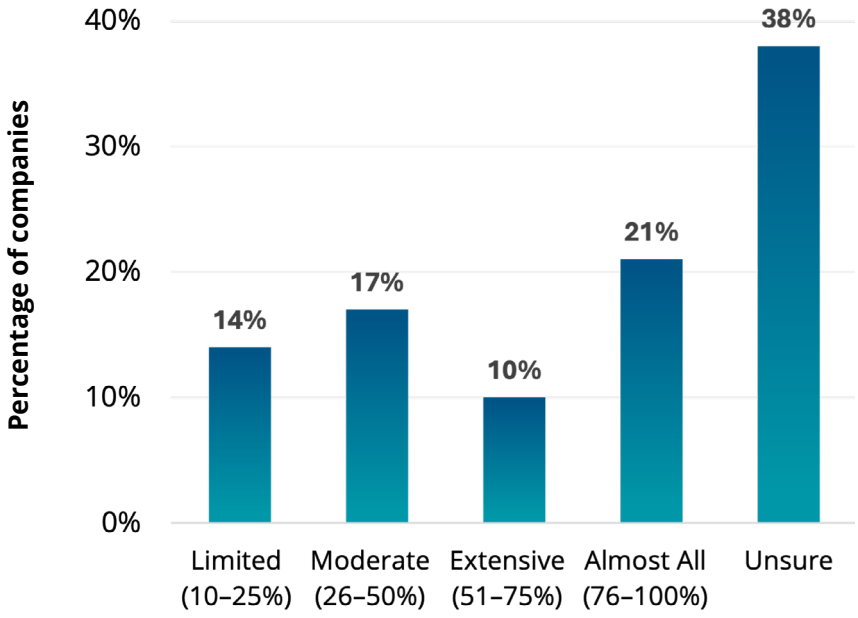
> The real magic happens when you have Cloud-native applications because that's where true auto-scalability happens
>
> **- Filipe Lucas, Global Head of Digital Services and Partner Management, EDP**

EDP capitalised on true efficiency through reconfiguring and re-architecting of applications to fully utilise Cloud-native capabilities. By adopting Cloud-native and serverless solutions, its applications automatically scale up or down as needed, ensuring continuous performance, even during periods of high demand. This Cloud implementation optimises resource allocation to applications, seamlessly allocating and deallocating containers, and virtual servers to adjust performance to peaks and lows, a vast efficiency improvement from manually installing and configuring virtualisation on a physical server.

European Companies Use Cloud to Improve Operational Efficiency and Automation

Operational efficiency is key for participants, which are therefore heavily focused on automating cloud processes, with more than 30% of the participants achieving very high levels of automation in deploying more than 50% of their cloud solutions to maximize efficiency. This automation is often boosted by AI and FinOps tools through enhanced pattern recognition and action triggers, which are increasingly adopted from the outset to optimize cloud costs and financial management.

Figure 7 – European companies automate the deployment process of cloud Solutions

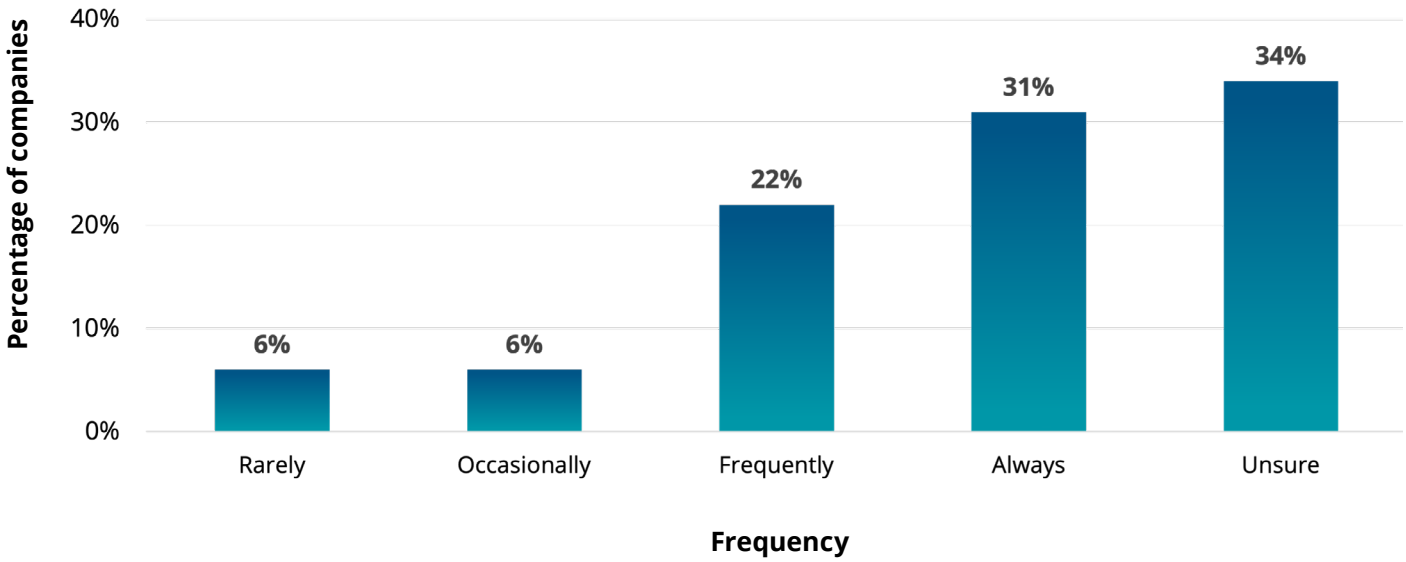


We built strong capabilities for a critical technology service that captures real-time data, improving the operational efficiency of our refinery representatives. Cloud services truly accelerated its deployment and innovation. Implementing this from an on-premises data centre would have been far more complex."

- Jean-Charles Hardouin, CIO, Arkema,
- Philippe Netzer-Joly, VP, Group Chief Cyber Security Officer, Arkema

A substantial 53% of participants frequently or always use cloud technologies to streamline their IT processes, which indicates a strong trend toward using cloud solutions like IaaS, PaaS and serverless computing to enhance business operations.

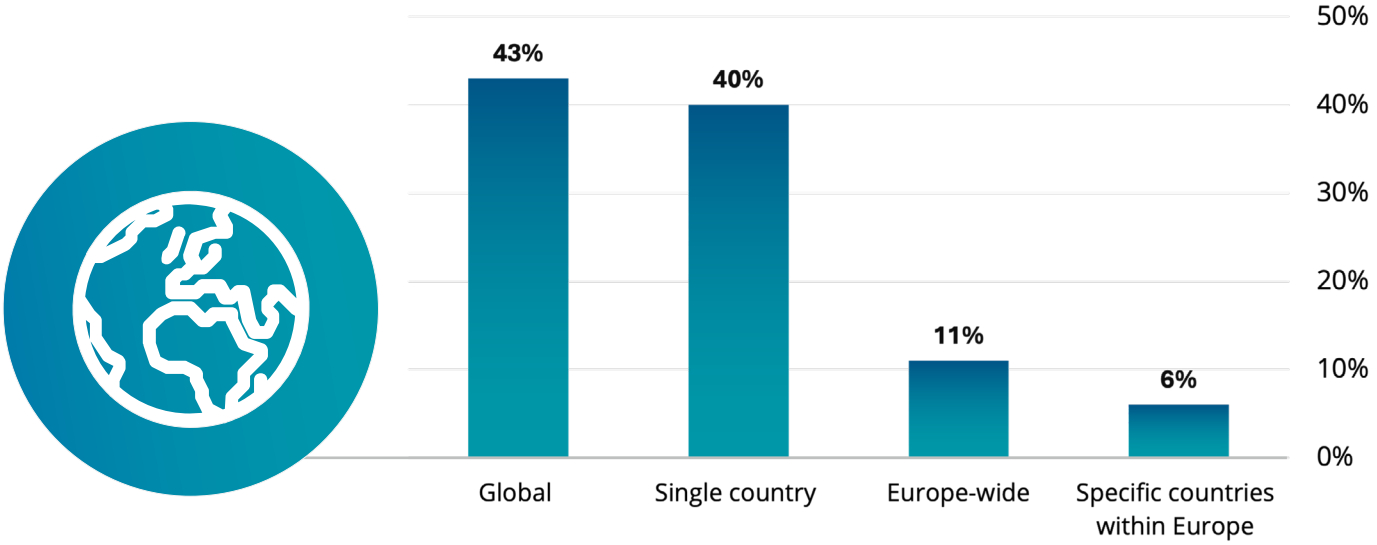
Figure 8 - Companies using cloud technologies (IaaS, PaaS, serverless infrastructure) to streamline their IT processes



European Companies Use Cloud to go Global

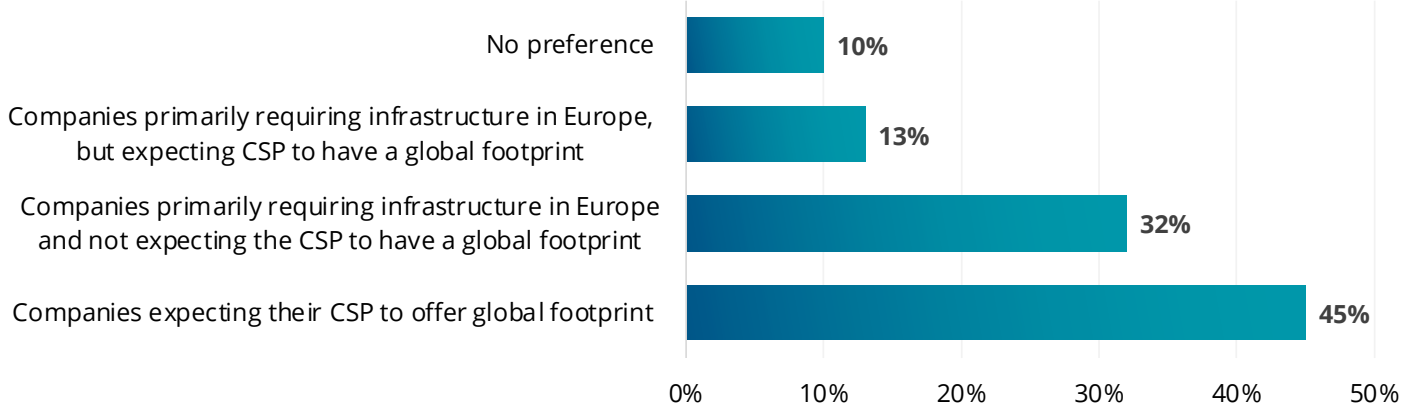
Cloud services are built upon extensive global networks of data centres, enabling participants to deploy applications and services closer to their end-users worldwide. This geographical distribution significantly reduces network latency, resulting in enhanced application performance and a superior user experience. 60% of the companies participating in the study are active in multiple countries, and over 40% have a global footprint.

Figure 9 - Participating companies operate in different regions



A majority, 55% of the total participants expect their cloud service providers to offer a global presence. For businesses with international operations or global customer bases, this is particularly relevant as it allows them to strategically position their cloud footprint and utilize specialized expertise wherever they need it around the globe.

Figure 10 - Companies require their cloud service provider to offer global footprint

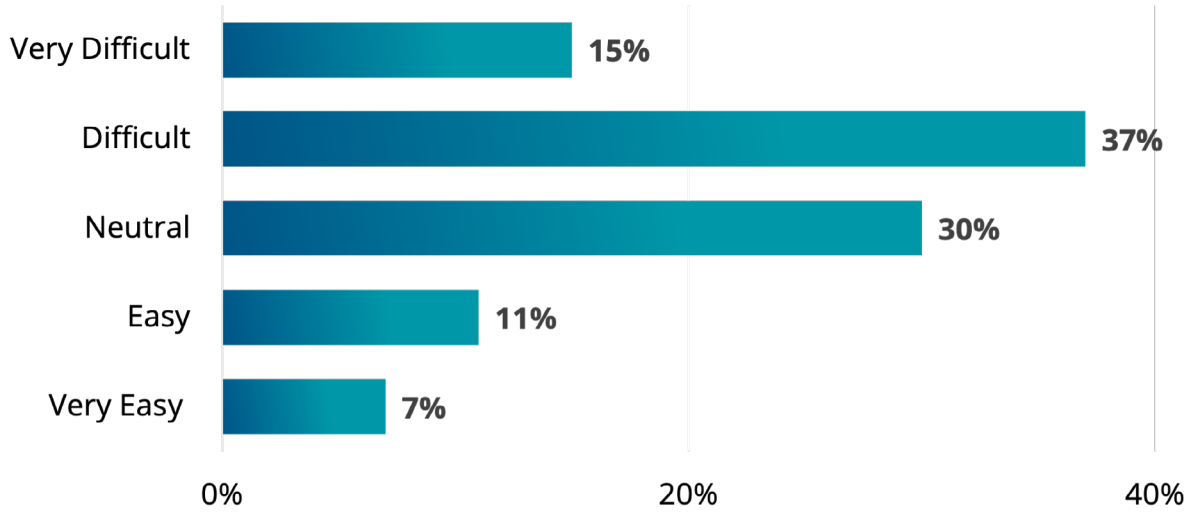


This global reach facilitates expansion into new markets without the need for physical infrastructure deployment in each region. A significant benefit of this model is the ability to leverage global talent pools. By using cloud services, companies can deploy workloads in regions where specialized expertise for managing cloud environments is readily available, a flexibility that would be impossible with traditional on-premises infrastructure. This strategic staffing helps manage and operate distributed cloud environments efficiently.

While finding professionals with general cloud knowledge is not a major issue within European countries, **52% of the participants stated that the true difficulty lies in sourcing candidates with highly specialized expertise**. This is particularly true for roles that combine technical proficiency with specific industry and domain knowledge, such as AI/ML, cybersecurity or FinOps.

> As a global company, we seek the best global technologies, including cloud service providers capable of delivering the solutions we need across our worldwide operations.
>
> **- Dimitrije Jankovic, Global Head of Digital Strategy and Operations, Sanofi**

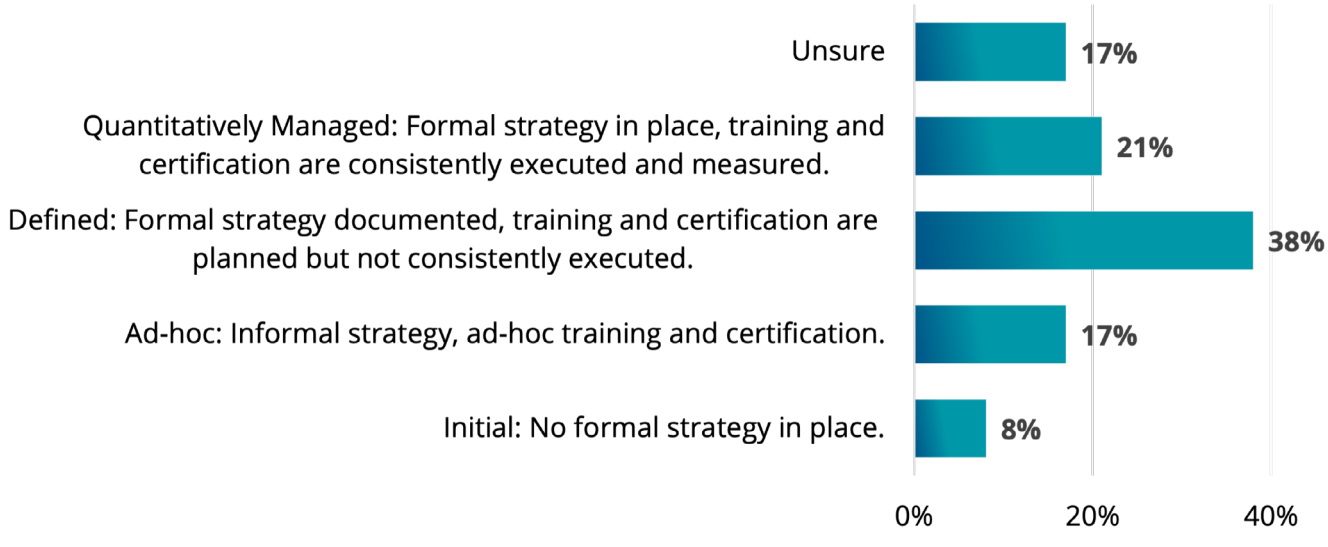
Figure 11 – Ease of finding qualified cloud personnel in Europe



> We constantly invest in training our developers on the latest cloud technologies. If you're afraid to train your own people, you'll not be able to retain your talent. You can't limit yourself by the fear of them leaving.
>
> **- Douwe de Vries, Engineering Manager and acting Head of Digital Technologies, NPO**

This skills gap has led many companies to rely on freelancers, consultants, or hybrid staffing models to meet their needs. There is also a broader concern that some European countries may struggle to find future IT and cloud skills, leading to calls for increased educational resources. To address these skill gaps, 59% of participants are investing in a formal strategy to train, upskill, and certify their current employees on cloud-related technologies.

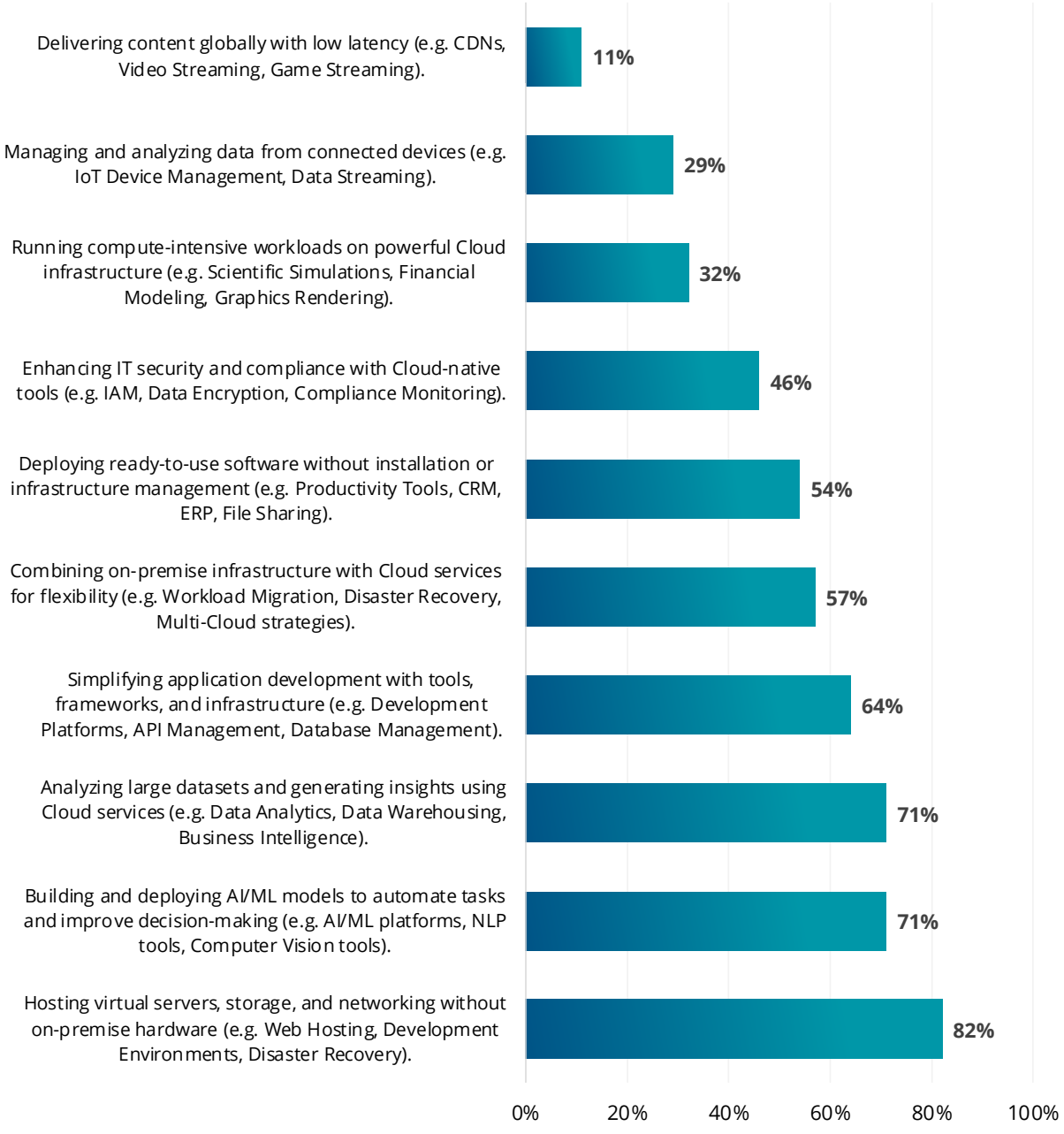
Figure 12 – Companies having a formal strategy for training and certifying developers, infrastructure teams and cloud-related roles



European Companies Use a Range of Cloud Services to Improve their Efficiency

European companies are primarily using cloud services for enhancing operational efficiency by hosting virtual infrastructure (82%), deploying AI and machine learning models for decision-making (71%), and analysing large datasets to generate business insights (71%).

Figure 13 – Primary usage of cloud services by European companies



> I don't think there's a single cloud service that we're not using. We have integrated cloud services, from security to the core of our imaging solutions.

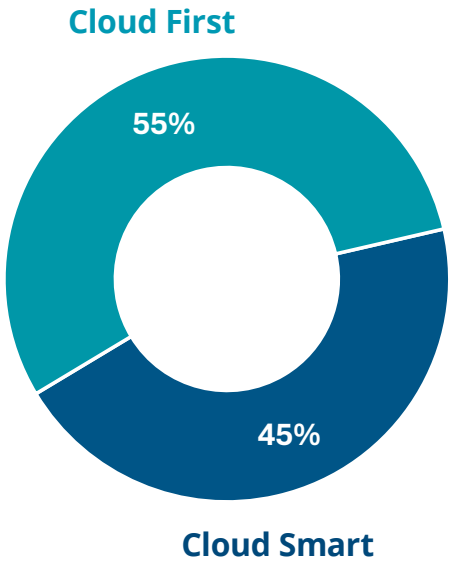
- Predrag Angelovski, VP, CTO at Healthcare Informatics, Philips

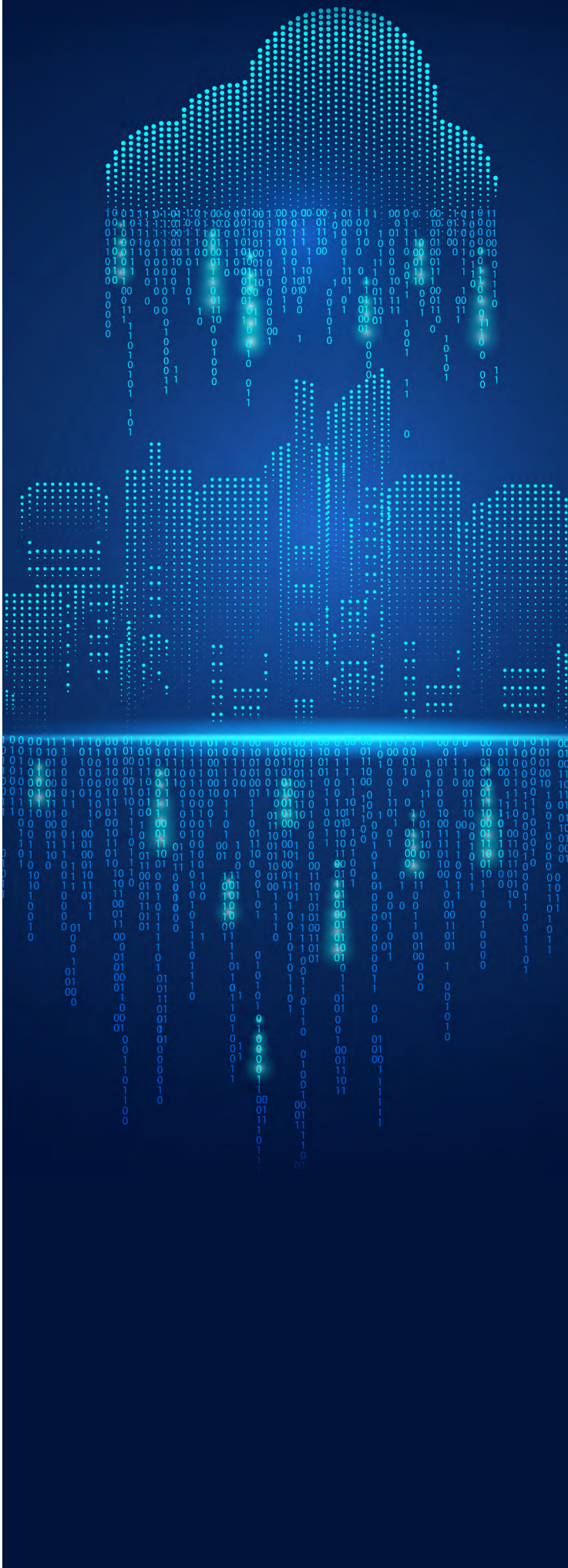
Philips is modernizing its traditional solutions, such as its integrated diagnostic solution, by using cloud services for hosting, computing, and storage. The company now leverages cloud technologies across its entire portfolio, utilizing managed services for solutions like the Radiology Operations Command Centre and other first-of-their-kind solutions. Philips's use of cloud extends from basic services like data storage and archiving to more advanced imaging services for storing, analysing, and managing metadata. They also rely on fully managed services from cloud providers to build, train, and deploy sophisticated machine learning models.

Cloud Strategy, Choice, and Satisfaction

This study shows that participants are using cloud computing in increasingly diverse and evolving ways, shaped by strategic priorities and workload needs. The study observed that companies choose different cloud adoption strategies, ranging from cloud First initiatives to more selective migrations. Two distinct archetypes have been identified that categorize how participants have approached the cloud. It is important to note that these approaches are sometimes mixed in practice.

Figure 14 – Percentage of companies following the two archetypes for their cloud strategy





First Archetype: Cloud First

The first archetype highlights the companies that have fully embraced a cloud First approach. For these participants, any new workload is designed and deployed as a cloud-first solution, prioritizing cloud infrastructure investments over on-premises capabilities. This strategy, seen across **55% of the participants**, utilizes the inherent agility and scalability of cloud environments for all new digital initiatives. This aligns with the broader trend[4] of most companies increasingly moving their workloads to the cloud, as the study's findings also show.

[4] Gartner - The Cloud Strategy Cookbook, 2023

Second Archetype: Cloud Smart

A second archetype involves a use-case driven approach, where **45% of the participants use the cloud based on specific business needs.**

This often manifests in two distinct ways: either in a structured manner with a clear distinction of which workloads and applications are suitable for cloud migration versus those that remain on-premises, based on specific functional needs and business cases. For instance, half of the cloud Smart participants select IaaS and PaaS solutions based on specific functional needs rather than an overarching cloud preference and decide to stay on-premises when there is no business case to move or develop a workload to cloud. In contrast, remaining companies select to move to the cloud in a more unstructured "opportunistic" manner, often reacting to immediate needs.

An important conclusion from the participants is the strong recommendation to move away from a simple lift-and-shift (IaaS-centric) approach. Instead, participants prioritize cloud-native development or application refactoring utilizing PaaS/SaaS solutions to truly capitalize on cloud benefits. This is because the unique requirements of certain applications, such as performance, latency, regulatory compliance, and security, necessitate a critical assessment to determine the optimal deployment model (public cloud, private cloud, on-premises, or hybrid).

Regardless of which strategy is adopted, cloud migration is typically a gradual process, involving a mix of basic refactoring and a focus on new cloud-native development to drive business value.

Multi-cloud Strategy

A clear trend in cloud adoption is the shift toward a multi-cloud approach. A significant 73% of participants have adopted this strategy and only 27% rely on a single cloud provider. Various third-party studies also support this finding.[5]

nterestingly, the path to multi-cloud varies. A notable 36% of participants began their cloud journey with a multi-cloud strategy from the outset. However, the majority (64%) made a strategic shift later to mitigate concentration risks and address the diverse needs of different business divisions.

> The world is hybrid. It's better not to rely on a single cloud provider. A multi-cloud strategy is better for financial competitiveness and business continuity.
>
> **- Jean-Charles Hardouin, CIO, Arkema**
> **- Philippe Netzer-Joly, VP, Group Chief Cyber Security Officer, Arkema France**

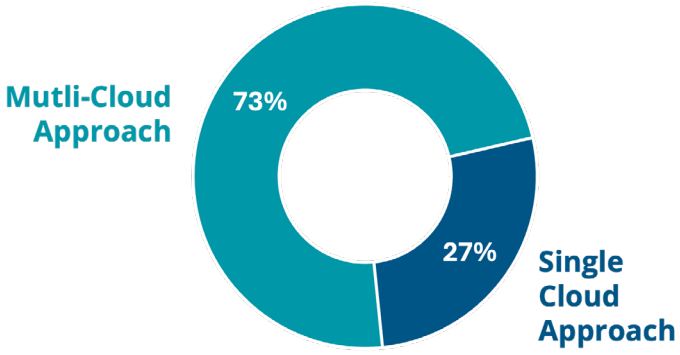
[5] Flexera report, 2025 (showing 87% of firms worldwide multi-cloud)
[5] Cockroach Labs survey, 2024 (50% across US, UK, Germany)
[5] OVHcloud survey, 2024 (62% in UK)
[5] Oracle survey, 2023 (98% globally)
[5] Public First survey, 2023 (71% in UK)
[5] Forrester report, 2022 (showing 87% of European companies use multi-cloud)

> Our cloud strategy evolved from single to multi-cloud to mitigate concentration risks and support our diverse divisional needs, such as existing investments in specific technologies for some divisions, and the need for advanced data analytics and AI capabilities for others. A third provider was preferred for its strong financial sector presence and specialized tools required by our clients.
>
> **- Peter Björnlund, Cloud Change Lead - Group CIO, SEB**

> We would rather use one global cloud service provider than assume the extra overhead of managing multiple local cloud service providers.
>
> **- Senior representative of a multinational healthcare company with annual revenues in the tens of billions of Euros**

Certain companies are even aiming to be explicitly cloud-agnostic, meticulously avoiding configurations that would hinder workload movement between providers to ensure maximum flexibility and competitive pricing.

Figure 15 - Proportion of single to multi-cloud companies



The rise of multi-cloud strategies remains a significant trend, driven by desires to avoid reliance on a single provider, utilize unique provider features, and benefit from competitive pricing.

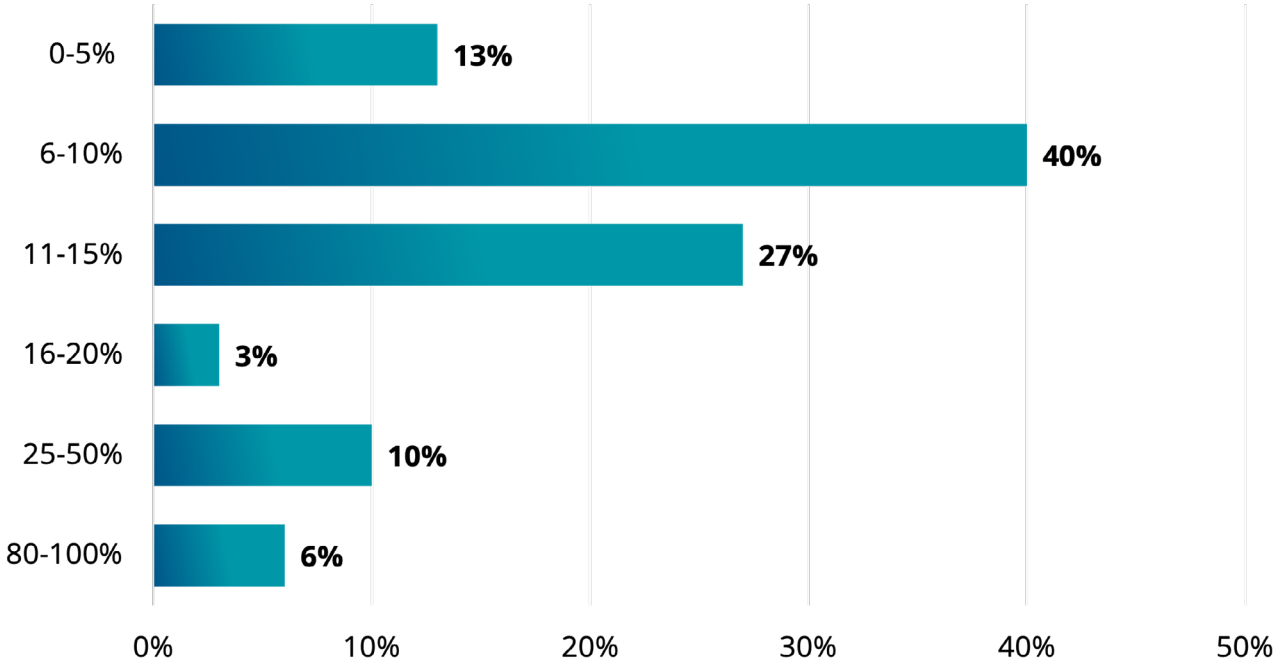
Despite noting the operational complexity that comes with switching and multi-cloud, the participants who adopted multi-cloud strategies suggest that they choose different providers for the competitive advantage of certain services, thus accepting technical differentiation across services as a normal effect of the competition among providers to offer innovative solutions. To make interoperability and switching easier for customers, providers are employing various measures including using open protocols, APIs, data formats and automation capabilities in their core services. This allows customers to build solutions that are inherently interoperable and transportable, effectively giving them the flexibility to be cloud-agnostic. Regulation recently entered into force - specifically the Data Act[6] - and AI tools are expected to further facilitate switching, interoperability, and the adoption of multi-cloud strategies. For example, technologies like Agentic AI have the potential to autonomously analyse and generate migration paths and optimize costs and act as a universal orchestrator across diverse cloud environments.

[6] The Data Act introduces rules to make it easier for users to switch between cloud service providers

Cloud Expenditure

A key finding of the study is that approx. **54% of participants currently dedicate less than 10% of their IT budget to public cloud infrastructure services while only 16% of participants dedicate more than 25%.** These figures fall below industry benchmarks for hosting, suggesting that a substantial volume of workloads remains within on-premises infrastructure. The study also found that cloud spending varies significantly by sector. Digital-native companies and those in fast-moving industries like fintech (80%) and media (20%) spend a much higher percentage of their IT budgets on the cloud. In contrast, sectors like healthcare (13%), financial services (12%) and transport (12%) are in the middle, while highly regulated industries such as public and defence (9%), telecom (8%) and energy (7%) spend less.

Figure 16 - Percentage of IT budget allocated to public cloud infrastructure.



Choice and Satisfaction of Cloud Service Provider

> If you want a stable, fully supported, highly secure, maintained, and operated platform for your production environment, you need a global provider.
>
> **- Søren Overholt Nicolaisen, Director of cloud infrastructure & Developer Experience, Novo Nordisk**

For the participants interviewed, selecting cloud service providers is not merely a technical choice; it's a profoundly strategic decision with far-reaching implications for their operations, innovation capacity, and market position. Participants consistently emphasized a multifaceted evaluation process, underscoring that their choice hinges on a careful assessment of several critical factors.

Breadth and depth of service offerings matter most for 78% of European companies interviewed

Foremost among the criteria for selecting cloud providers is the breadth and depth of service offerings. Aligned with the cloud adoption strategies earlier presented, participants rigorously assessed the comprehensive range of services available from each cloud service provider (CSP), from foundational compute, storage, and networking to more advanced, specialized capabilities such as machine learning, artificial intelligence, and IoT as the choice of CSP – whether structured or unstructured – depends on the services which companies can use from the provider. The ability of a provider to offer a broad range of tools and functionalities was paramount, ensuring that current and future technological needs could be met within a single platform or a carefully curated multi-cloud environment. 78% of the respondents indicated that their initial evaluation strongly prioritized providers demonstrating extensive scope of services. These services included key capabilities such as scalability, flexibility, access to innovation, strong performance, robust cybersecurity, and access to advanced technologies like AI and data analytics. This strategic evaluation then led companies to carefully select which workloads reside on which cloud, based on best-of-breed solutions. This approach involves choosing specific providers whose services excel in particular areas, thereby optimizing performance, cost, and accelerating speed to market.

When discussing breadth and depth of services, companies highlighted their preference for using CSP for their distinct strengths, from cloud-native focus, extensive AI services, advanced machine learning and analytics tools, to comprehensive service suite and deep compatibility with existing enterprise systems. The consensus among participants was that global CSPs offer a broader breadth and depth of services, covering everything from basic compute and storage to complex managed databases; however, the preference often hinged on a case-by-case basis, dependent on the type of workload and required services.

A majority of participants (76%) agreed that global CSPs offer higher quality services than their EU-based counterparts. This includes quality in terms of diversity of advanced services including AI/ML, data analytics, and high-performance computing.; a majority of the participants made it clear that they would expect comparable service levels and cost-effectiveness from European providers and would not be early adopters until then.

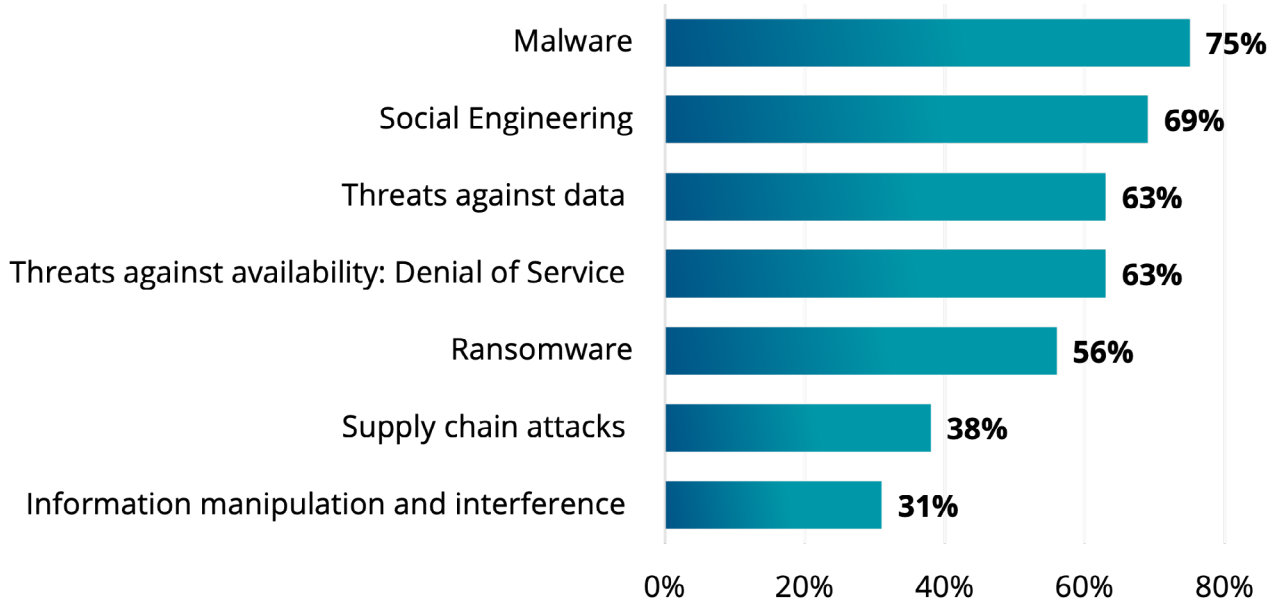
Enhanced security and compliance with regulations is prioritized by 41% of companies interviewed when choosing a cloud provider

Equally critical are the CSP's capabilities in navigating complex regulatory landscapes. **In an increasingly regulated global environment, 41% of the participants prioritize providers that demonstrate a robust understanding of, and proactive adherence to, diverse national and international compliance frameworks**.

This includes not only general data protection regulations but also industry-specific mandates and considerations around data residency and sovereignty. Participants sought assurance that their chosen CSPs could help them meet these stringent requirements, mitigating legal and reputational risks.

The ENISA 2024 Threat Landscape Report[7] identified seven prime cybersecurity threats in the European Union, which most participants consistently experienced throughout the year.

Figure 17 – Cybersecurity Threats faced by European companies



A significant 72% of participants indicated that they view certain global CSPs as having a proven ability to help them both navigate complex regulatory landscapes currently and offer the most appealing solutions to current cybersecurity threats.

[7] ENISA - Threat Landscape Report, 2024

The quality of customer support is vital for 30% of participants

The perceived quality of customer support was consistently cited as a vital factor for a positive experience by 30% of the participants. Beyond technical features and compliance, participants place high value on the responsiveness, expertise, and dedication of a CSP's support teams. Access to technical account managers, comprehensive documentation, and various support plans were all seen as crucial for addressing issues, facilitating learning, and ensuring smooth operations, ultimately contributing to a positive overall experience. Beyond customer support, participants are looking for true business partners; hence CSPs aligning with their specific strategic objectives, whether that means fostering innovation, ensuring seamless integration with existing enterprise systems, or meeting stringent data sovereignty requirements.

Flexible pricing options and cost transparency are key factors for 39% of the companies interviewed

Pricing emerged as a significant consideration for 39% of participants. While the allure of cloud elasticity often implies cost savings, approximately half of the participants highlighted the complexity involved in understanding and managing cloud expenditure. They scrutinize the granular pricing structures, looking for transparency and tools that enable effective cost optimization and forecasting. The ability to control and predict cloud spending was a key driver in their evaluation process. High unexpected costs may arise if participants do not apply such procedures and mechanisms.

A very high level of satisfaction was reported with certain global CSPs, seen as currently offering a more comprehensive package for cost management and optimization, supported by their reliability, redundancy, and scalability. While participants acknowledged the complexity of the pricing models, they found that global providers consistently offered more extensive tools to manage these costs.

Finally, participants provided insights into overall satisfaction. Satisfaction with Global CSPs remains very high, with 91% of participants reporting they are satisfied or highly satisfied. This high satisfaction was largely attributed by participants to their operational efficiency, resilience, and comprehensive support.

27% of Participants are Concerned About Digital Sovereignty and 10% have Started Looking into Sovereign Cloud Solutions

Heightened geopolitical uncertainties are a growing concern for many of the participants, but a much smaller group (less than 10%) has actually begun to prepare contingency plans, e.g. rebalancing workloads toward on-premises infrastructure.

On this backdrop, digital sovereignty is a concern for 27% of the participating companies, with some of them (10%) already looking into sovereign cloud solutions and analysing whether the business case and cost impact would justify digital sovereignty as a primary requirement for changing their cloud procurement strategy.

According to the European Public cloud IaaS 2024 Vendor Assessment by IDC and Deloitte cloud Sovereignty report [1], the current market in Europe of sovereign cloud services is growing, with both global and European cloud providers developing offerings tailored to European needs that emphasize assurances for customer control over data and confidence regarding service continuity.

> Amidst evolving global dynamics, cloud service providers cater for uncertainties and actively reassure clients as reliable partners, working towards shared objectives.
>
> **- Stijn Lehaen, CTO, VRT**

Cloud Regulatory Landscape

We believe technology must be used responsibly and ethically. Regulations are crucial for defining these boundaries, especially concerning the ethical use and access of data, AI, and technology. Regulations are there to make sure innovation goes at a reasonable pace. Our hope is for regulations to evolve as rapidly as technology. The real challenge often lies in their application and the varied interpretation; they are often applied and interpreted differently across different countries, creating complexity for everyone involved.

- Predrag Angelovski, VP, CTO at Healthcare Informatics, Philips

While a regulatory framework and clear guidelines are essential, and understanding them has become part of our job, the concern lies in the shift from a unified European framework to individual countries pursuing different approaches. This creates unnecessary overhead and complexity, somewhat defeating the purpose of having a European standard in the first place.

- Senior representative of a multinational healthcare company with annual revenues in the tens of billions of Euros

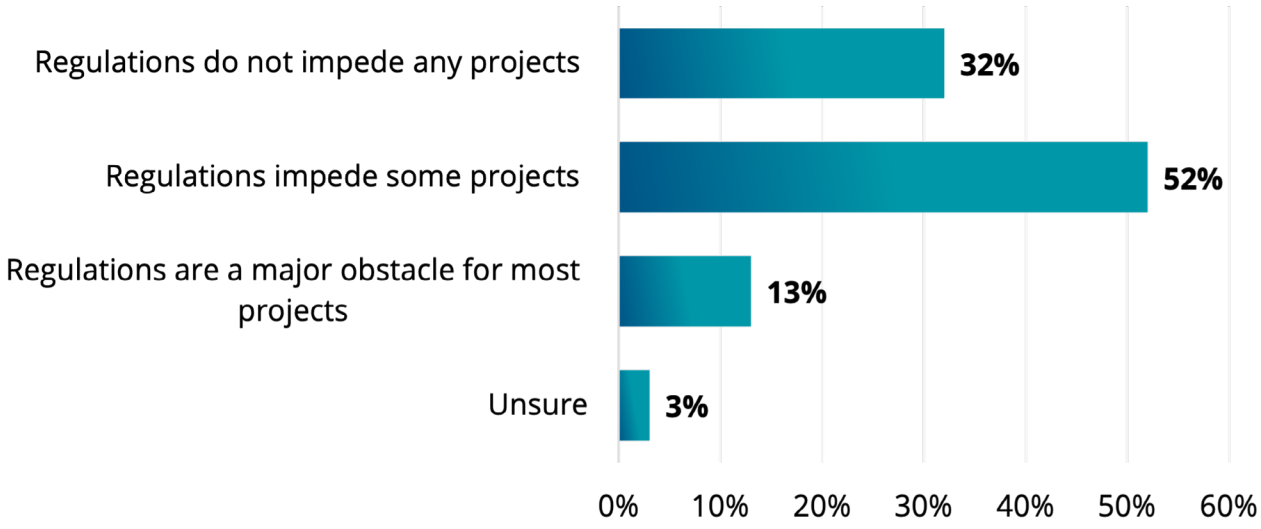
The perspective on regulatory compliance

EU Regulations

EU regulations present a challenge and opportunity for companies adopting the cloud. **A significant portion of companies experience compliance with EU regulations as a substantial burden. In fact, 65% of participants recognize it as such, including 13% considering it a major obstacle for certain projects**. These frameworks are said to demand substantial investments and engineering efforts for compliance, often increasing time-to-market and acting as obstacles to creating a mature market in the EU. Examples of particularly impactful regulations cited include GDPR, NIS2, DORA, CRA, EU Data Act, EU DPR, EAA, and the EU AI Act[8], alongside various local and industry-specific laws, and specific data warehouse standards or GXP compliance in healthcare. The impact is felt through limitations on using certain cloud providers or technologies due to regulations like EUCI, difficulties integrating compliance requirements with legacy systems, and restrictions on placing highly sensitive data or data impacting critical infrastructure in the public cloud.

32% of the participants say regulatory compliance can sometimes act as an enabler for digital transformation and cloud adoption, by motivating companies to actively enhance their IT maturity and security, which can ultimately lead to overall cost reduction. This sentiment is stronger in heavily regulated sectors like financial services and energy. Participants in these industries appreciate that stricter regulations protect their interests and acknowledge the critical importance of frameworks like GDPR, DORA and NIS2. Larger companies with a strong capacity to organize for compliance, often believe that investing in prevention is better than facing security or legal consequences.

Figure 18 – Perspective on regulatory compliance as an obstacle to Cloud adoption



[7] See details of the specific regulations in the Regulations repository section

Non-EU Regulations

Operating in a globalized market requires European companies to navigate a complex and often overlapping international regulations regarding data residency and privacy, forcing them to dedicate significant resources to compliance strategies for international data transfers (for instance the National Data and cloud Policy in South Africa, Brazil's LGPD (Lei Geral de Proteção de Dados), or the PDPL (Personal Data Protection Law) in Chile). Due to lack of global agreements, the trend is moving towards isolationist policies rather than a unified structure. Crucially, major CSPs enable their clients to navigate these complex regulatory environments.

The US CLOUD Act[9] is an example of a non-EU regulation that has extraterritorial reach. It applies to a broad range of online service providers with operations in the U.S. and was created to address challenges law enforcement agencies faced in obtaining data stored abroad in cross-border investigations involving serious crimes. When asked whether participants are aware of this legislation, 62% responded affirmatively.

Among the 62% who were familiar with the cloud Act, 31% believe lawful requests from law enforcement can be challenged in court if they conflict with the laws of the country where the data is stored. These participants remain cautiously optimistic, trusting in cloud providers' commitment to defend against unjustified or overly broad data access requests in US courts. 15% believe that data requests under the cloud Act are targeted at serious crimes and must be specific, relevant to an investigation, and approved by a court, hence it's not a major concern for them. Another 15% believe that even if US authorities were granted access to data under the act, their encrypted data stored with cloud providers would remain unreadable, especially when using customer managed keys, and envelope encryption. 15% of this group assume European providers are not subject to US law and therefore are better positioned to protect data from law enforcement requests under the cloud Act, while only 8% recognize that the cloud Act applies to any CSP that operates or has a legal presence within the US, including the European CSPs.

It is worth noting that CSPs regularly publish transparency reports[10,11] on law enforcement access, showing a very low number of requests that have resulted in the disclosure of EU customer content data over time. This gives a strong indication that the risk is low. This record also partially reflects the nature of law enforcement investigations which primarily focus on collecting electronic evidence from consumer/individual accounts.

[9] https://www.justice.gov/criminal/cloud-act-resources
[10] Microsoft - Government Requests for Customer Data Report
[11] AWS has not disclosed any enterprise or government customer content data under the CLOUD Act since 2020

Impact of regulations on innovation

Almost a third of the participants report that due to regulations, EU companies are lagging behind in terms of technology and innovation. Regulations like the EU AI Act and Cyber Resilience Act, despite their good intentions, are considered counterproductive by some, increasing complexity and costs. It is argued that these Acts prevent European participants from taking advantage of the latest features and fully utilizing AI compared to other regions, hampering innovation and requiring extensive legal discussions before integrating new services. Participants generally agree on the need for governance to ensure the responsible use of AI. However, there is concern that over-regulation of these evolving technologies poses a significant challenge for companies seeking to benefit from them. As one participant noted, the shift from a guidance-based framework to strict, prescriptive regulation makes cloud and AI adoption both complex and difficult. The core challenge lies in the lack of clarity between a mandatory rule and a recommendation, which can impede adoption. This creates a challenging environment for European participants to compete on a global scale, highlighting a critical need for regulatory harmonization on European or international level.

For 45% of participants, regulations are sometimes introduced too soon, suggesting that companies should be allowed to first adopt and utilize new technologies before comprehensive regulations are applied. This situation has led some participants to consider migrating certain tasks to other regions or performing Proofs of Concept (POCs) in less regulated countries outside the EU to optimize investment and remain compliant. For example, a company might conduct its initial AI model testing in a country with fewer regulations to validate its effectiveness before committing to the substantial costs and engineering efforts required to meet the strict requirements on data transparency, algorithm explainability, and bias mitigation for an EU rollout. **Overlapping and conflicting regulatory requirements across different jurisdictions are a significant barrier to cloud adoption**. This regulatory fragmentation leads to a proliferation of uncoordinated data residency and transfer requirements, creating substantial operational complexity and cost for any cross-border data movement.

When it comes to navigating this complex regulatory landscape, most participants preferred Global CSPs.They are frequently cited as the most capable providers in supporting customers across multiple jurisdictions, thanks to their extensive experience in understanding customer needs and robust infrastructure. They offer a comprehensive suite of features that address key EU compliance requirements, including a wide array of global data residency options, compliance certifications, data masking, enhanced security measures and powerful audit and reporting tools. These CSPs offer various forms of support, including dedicated personnel, helpdesks, or white papers, to help customers better understand and comply with regulations.

Escalating compliance costs and their impact

The overall financial burden of regulatory compliance presents a diverse picture. **A significant 60% of participants expressed dissatisfaction with current compliance costs, while the remaining view it as a necessary investment to protect their interests.**

Beyond the quantifiable expenses, the true cost of compliance often lies in less tangible yet highly significant areas. These costs manifest as lost opportunities, such as the inability to effectively take advantage of AI or expand into new markets. To emphasize this point, a participant classified the current regulatory approach as "creating borders before knowing the size of the field". This sentiment was also echoed by CIOs and CTOs of global companies, who noted the **lack of clarity in interpreting and applying regulations like GDPR. Individual countries often translate these rules differently, creating their own local variations**, or have their own separate rules, for example C5 and BDSG in Germany or HDS and INS in France for the healthcare sector etc. This defeats the purpose of having a single EU standard, leading to significant overhead and complexity. As a result, certain companies are forced to establish new offices and hire personnel in multiple countries or even rebuild their products to comply with different national interpretations. This significantly inflates development, deployment, recruitment, and training costs even before a product enters the market. Such a heightened regulatory burden, particularly in the EU, also contributes to a slower pace of innovation compared to less regulated counterparts.

> The cost of regulatory compliance is very high. For anything involving AI, human oversight is mandatory, requiring trained individuals for continuous monitoring and risk assessment. This is a massive undertaking to provide regulatory support, and while large companies can hire specialized talent, smaller companies might find themselves basically lost in their innovation journey
>
> **- Søren Overholt Nicolaisen, Director of Cloud Infrastructure & Developer Experience, Novo Nordisk**

Looking ahead, **the agreement among (76%) participants is that regulatory compliance costs will continue to climb in the short term**, with none of the respondents believing costs will decrease. This consensus aligns with historical data, underscoring a consistent and sustained growth in compliance expenditure. Many anticipate a continued ascent as new regulations, like DORA and NIS2, frequently augment existing requirements. While some foresee a stabilization in the long run, the prevailing strategy to mitigate rising costs involves building smart, resilient, secure systems that are architected to adapt seamlessly to regulatory requirements.

Figure 19 - Perspective on current cost of regulatory compliance required for digital transformation, cloud and AI adoption in Europe

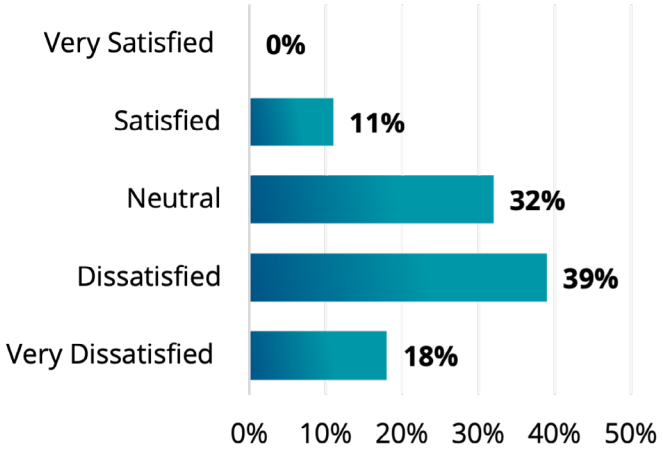
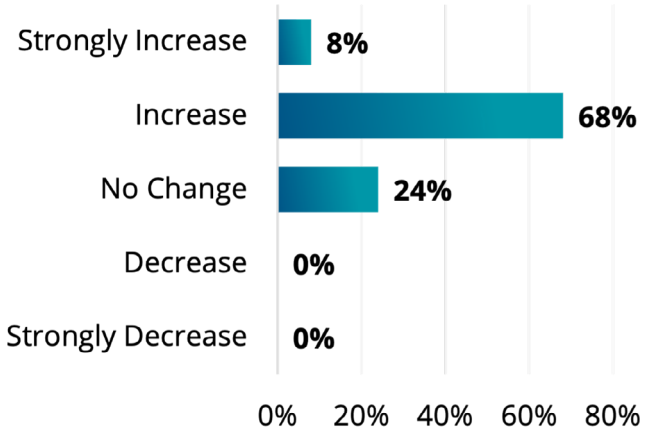


Figure 20 - Current compliance costs and future outlook

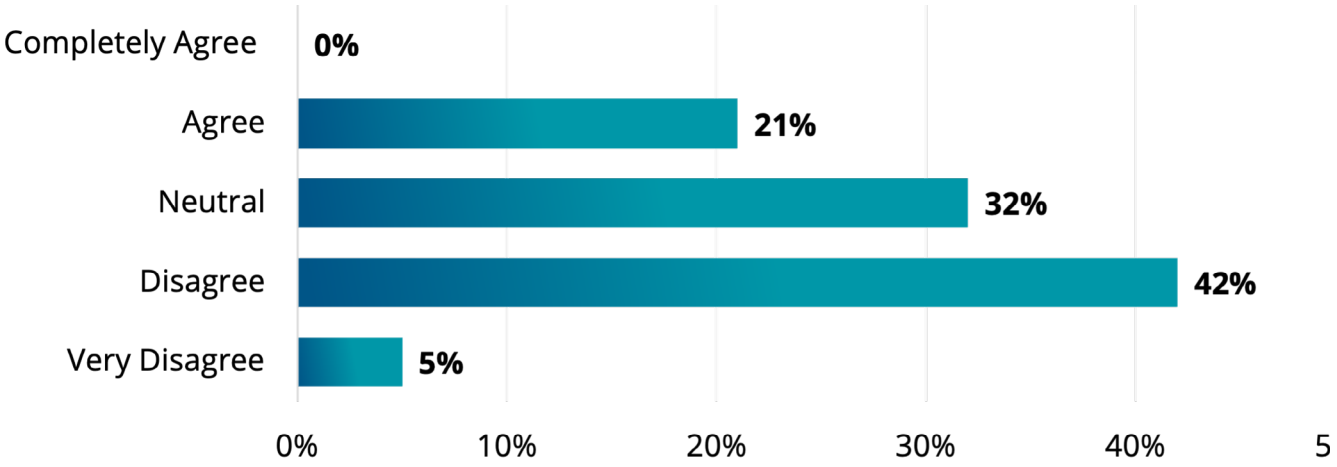


Companies' recommendations

There is a consensus among the participants that clear, harmonised European regulations are essential to accelerate digital innovation and cloud adoption. As aforementioned, the current fragmented regulatory environment, with different interpretations of European regulations across different countries, creates complexity and increases costs for participants striving for compliance. Despite these challenges, Europe remains a prevalent geography for participants and remains a key pole of investment. Participants warn, however, on the outlook of the said investments when considering the state of regulations. This is supported by the fact that **47% of the participants consider Europe's regulatory environment less attractive for their next strategic investment**. Customers did note, however, that CSPs compliance capabilities are consistently improving, which is viewed as a very positive development. This improvement offers companies much-needed reassurance that CSPs are actively evolving to meet their regulatory requirements. In the healthcare sector, there is a strong urge for regulators to balance innovation and risk control, as **more than 80% of participants in healthcare view current regulations as slowing down the pace of innovation**, highlighting the need for faster processes to bring life-saving products to market.

While **there is a broad consensus among CIOs and CTOs that the concept of digital sovereignty requires clarification,** opinions diverge on the appropriate level. The participants' views are split almost evenly between a desire for international standards and a focus on European-level regulation that defines technical and organizational measures to ensure cloud customers retain full control over their data.

Figure 21 – Is the EU's regulatory environment attractive for next strategic investment?

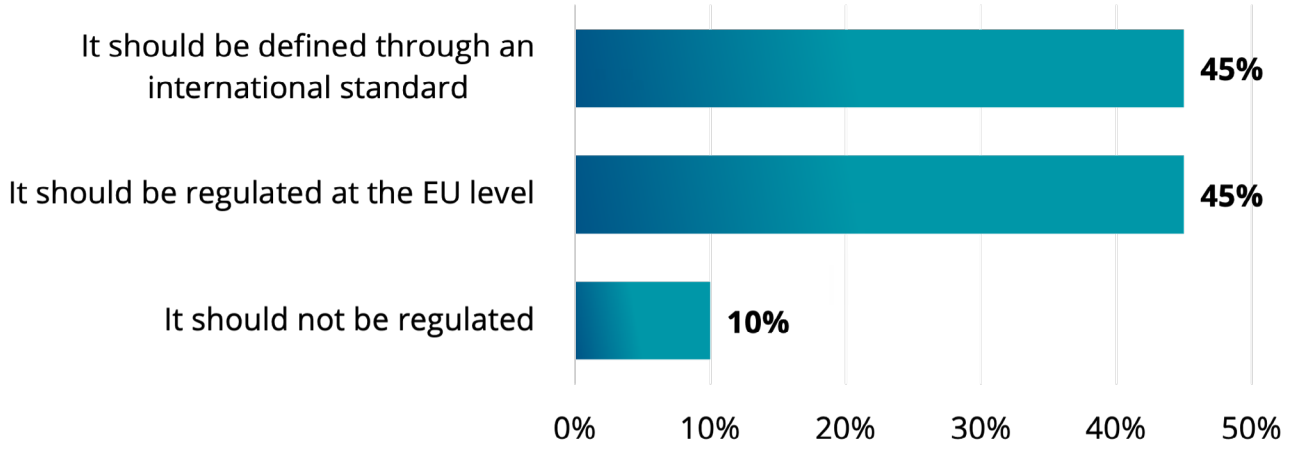


Approximately 45% of participants believe the ideal solution lies in a unified international standard. However, this group also expressed scepticism about the feasibility of an international alignment on a common approach to sovereignty requirements. An equally large group **(45%) advocates for European-level regulation**, as a set of technical, contractual and organizational measures that ensure customer control over data location, access, encryption, and resilience. 10% of participants believe that digital sovereignty should not be regulated at all. They argue that it should be left to individual customers to determine their own risk tolerance and define the necessary contractual and technical requirements for providers.

Participants who expressed their view highlighted that data sovereignty should evolve beyond a country/region-level approach towards multilateral agreements, such as between the EU and China, or the EU and the US. They expect the European Commission to prioritize fostering this type of international cooperation and continue to actively engage with EU CIOs to develop proposals that stimulate this discussion. **They advocate for harmonization of regulatory frameworks (e.g., cybersecurity, AI), allowing companies to experiment and innovate to support the growth of the European digital economy. This quest for harmonization was explicitly shared by 80% of the participants**. There is a general push for less localized and more harmonized regulations and standards, either at the EU or international level. For instance, companies in the healthcare sector believe that unified global database offers invaluable advantages to medical research and innovation leading to better healthcare outcomes.

Participants expect that this approach would facilitate trade and investment by creating a more predictable regulatory environment, enhance efficiency by reducing redundant compliance requirements, lower compliance costs, and promote innovation by providing clearer guidelines and standards. By aligning regulations across different regions and sectors, harmonization can create a more cohesive and supportive framework to reap the benefits of cloud technology.

Figure 22 - Perspective on regulating digital sovereignty



Conclusions

This report underscores a profound transformation in cloud computing, moving beyond mere technological adoption to a strategic imperative that redefines business operations and competitive advantage. The journey to the cloud is driven by an undeniable need for agility, speed, and scalability, enabling participants to innovate rapidly and respond dynamically to market shifts. cloud services are vital in the way large European companies in critical sectors use cloud computing for accessing cutting-edge technologies like AI/ML, optimizing overall costs through efficiency gains, and building highly resilient, secure global infrastructures that ensure business continuity.

The companies and public sector organizations that we have interviewed for the study are approaching cloud adoption with increasing sophistication, embracing diverse strategies from "cloud First" to "cloud Smart" approaches. Even if the use of multiple providers may introduce operational complexities and need for stricter cost management, the rise of multi-cloud strategies remains a significant trend, driven by desires to avoid reliance on a single provider, utilize unique provider features, and benefit from competitive pricing. A significant trend is the rise of multi-cloud strategies, driven by desires to avoid reliance on a single provider, utilize unique provider features, and benefit from competitive pricing. In addition, a critical understanding has emerged that despite understanding the benefits of cloud computing, most companies dedicate less than 10% of their IT budget to the public cloud infrastructure services. These figures fall below industry benchmarks for hosting, suggesting that a substantial volume of workloads remains within on-premises infrastructure. This can be due to regulatory requirements, latency needs, or simply lack of business case for cloud use for certain workloads. The IT budget is expected to shift more toward the cloud in the coming years.

The selection of cloud service providers is a strategic decision, with breadth of service offerings, regulatory compliance, pricing transparency, and quality of customer support being paramount. Global CSPs maintain very high satisfaction due to their ability to deliver on these expectations, as well as due to their operational efficiency and comprehensive support. Digital sovereignty is not yet a primary driver for CSP selection, but it is a topic that European companies are looking more into.

The regulatory environment further complicates matters, simultaneously enabling IT maturity and imposing substantial burdens that can stifle innovation and increase compliance costs. There is a strong call for harmonizing existing regulations in adherence to international standards to balance innovation with risk control ultimately fostering digital growth and investment globally.

In conclusion, the path forward for cloud adoption in Europe requires a proactive and collaborative approach. While companies are clearly aware of the strategic benefits and are increasingly leveraging multi-cloud environments, their progress is often constrained by a fragmented regulatory landscape. To fully realize the transformative potential of cloud computing, regulators must work closely with the industry to establish a harmonized framework that promotes clarity and predictability based on choice of provider. This will be essential for meeting important policy objectives, including digital sovereignty, data protection and competitiveness and ensuring Europe can strengthen its position as a global leader in the digital economy and remain a favourable destination for foreign investments. The ability to effectively address these challenges will determine whether the cloud becomes a true catalyst for European growth and is able to unlock its full potential.

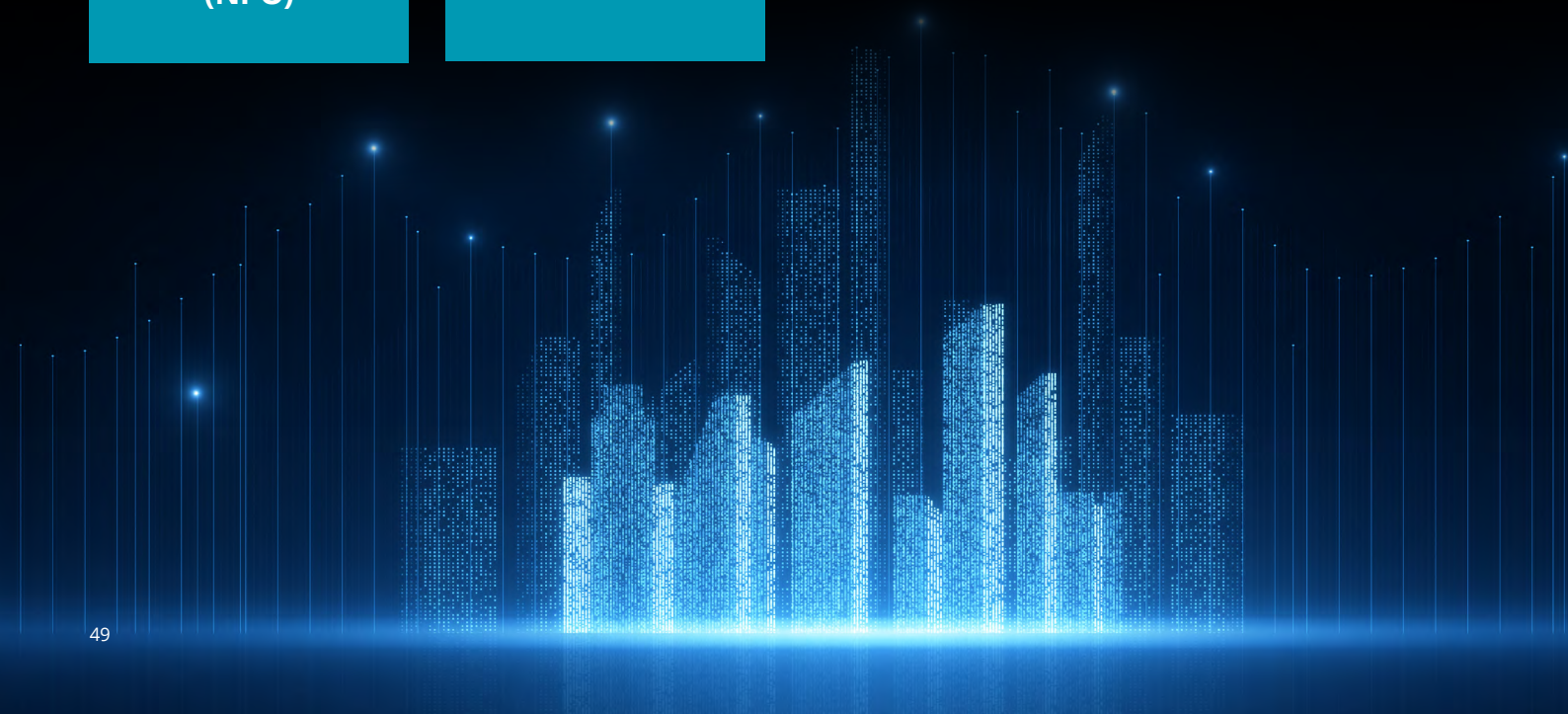
Regulations Repository

- BDSG (Bundesdatenschutzgesetz): German law regulating how personal data is processed to protect individual privacy and data security.
- CRA (EU Cyber Resilience Act): EU regulation setting cybersecurity requirements for digital products to ensure their security throughout their lifecycle.
- DORA (Digital Operational Resilience Act): An EU regulation strengthening the digital operational resilience of the financial sector against cyber threats.
- EBA Outsourcing guidelines: European Banking Authority guidelines ensuring financial institutions manage risks from outsourcing activities.
- EAA (European Accessibility Act): EU directive that sets mandatory accessibility requirements for a wide range of products and services, aiming to make them more accessible to people with disabilities.
- EU Data Act: EU regulation creating rules on who can access and use data generated by connected products.
- EU DPR (Data Protection Regulation for EU Institutions, Bodies, Offices and Agencies): EU regulation protecting personal data processed by the bloc's own institutions and bodies.
- INS (Identifiant National de Santé): A unique, permanent health identifier for French citizens used by all healthcare professionals to securely share data.
- EU AI Act: A new EU law regulating AI systems based on their potential risk to public safety and fundamental rights.
- EUCI (European Union Classified Information): Regulations protecting sensitive information whose unauthorized disclosure could harm EU interests.
- FDPA (French Data Protection Act): French law providing a framework for data protection and individual rights, aligning with GDPR.

- GDPR (General Data Protection Regulation): EU regulation protecting the personal data and privacy of EU citizens.
- GXP compliance: Quality assurance regulations for regulated industries to ensure products are safe and meet quality standards.
- HIPAA (Health Insurance Portability and Accountability Act): A U.S. law protecting the privacy and security of individuals' medical information.
- ISO 27001: International standard for an Information Security Management System (ISMS) to manage information security risks.
- NIS2 (Network and Information Security 2 Directive): An EU directive achieving a high common level of cybersecurity across the EU.
- PCI (Payment Card Industry Data Security Standard): Security standards for organizations handling payment cards to reduce the risk of fraud.
- SOC 2 (System and Organization Controls 2): A report attesting to how a service organization manages security, availability, processing integrity, confidentiality, and privacy based on applicable trust service criteria.
- C5 (cloud Computing Compliance Criteria Catalogue): A German standard providing a security framework for cloud service providers.
- ENS (Entry Summary Declaration): A customs document providing advanced information on goods entering the EU for security and safety risk assessment.
- HDS (Hébergeur de Données de Santé): A French certification for health data hosting providers ensuring patient data security and confidentiality.
- Cloud Act (Clarifying Lawful Overseas Use of Data Act): U.S. law clarifying the authority of U.S. law enforcement to request data from service providers in a criminal investigation, regardless of where the data is stored globally, and enabling reciprocal agreements with foreign governments to streamline cross-border access to electronic evidence for serious crime investigations.

Participating Companies

Autostrade per l'Italia	Sanofi	Philips	EDP
Stripe	Naturgy Energy Group	Skandinaviska Enskilda Banken (SEB)	Arkema
Amadeus IT Group	Belgian Post Group (bpost)	Credendo	CETIN
Seguros Santalucía	Roche Diagnostics	Vlaamse Radio- en Televisieomro-eporganisatie (VRT)	Radio-télévision belge de la Communauté française (RTBF)
Nederlandse Publieke Omroep (NPO)	Volkswagen Group Polska		



Participating Companies (Cont.)

- Market-leading telecom provider in a major European country with multi-billion-euro revenue
- One of the largest associations of cooperative banks in Central Europe
- Large Retail and Wealth management bank in the Nordics with AUM in billions of euros
- One of the oldest commercial banks offering banking and financial services in Nordics
- Global logistics provider with annual revenue in billions of euros
- Large International Public Sector Organization
- Multinational pharmaceutical company employing tens of thousands of people
- One of the largest stock exchange groups in Europe with presence in capital markets and digital currency business
- Leading biotech company optimizing clinical trials and developing AI diagnostics
- One of the largest electricity producer and supplier in South-eastern Europe with revenue in billions
- Leading defence institution
- Prominent space organization
- Information technology and electronic communications services provider for energy sector with revenue in billions
- One of the largest providers of healthcare services in Nordics with tens of thousands of employees

Authors

This report has been set up by :

Thomas Kessler
Partner
Cloud Strategy and Architecture
thkessler@deloitte.com

Bram De Schouwer
Partner
Cloud Strategy and Architecture
bradeschouwer@deloitte.com

Aurélien Descamps
Director
Cloud Strategy and Architecture
audescamps@deloitte.com

Cedric De Schepper
Senior Consultant
Cloud Strategy and Architecture
cdeschepper@deloitte.com

Deloitte.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, tax and legal, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte has in the region of 312,000 professionals, all committed to becoming the standard of excellence.

MAKING AN IMPACT THAT MATTERS since 1845