KPMG

Cloud Monitor 2025

Digital sovereignty begins in the cloud - how companies create innovation, security and trust

Study, September 2025

Contents

Foreword

Cloud computing has finally become a business-critical foundation in 2025. The Cloud Monitor 2025 shows that companies are now aligning their cloud strategies strictly with goals such as agility
digital sovereignty and cost control. Hybrid architectures dominate, with a clear trend towards the public cloud. Cloud-first strategies continue to gain in importance. At the same time, companies are anchoring multi-cloud concepts in order to reduce dependencies and keep innovation paths open.
At the same time, the demands on providers are increasing: performance, security and compliance are no longer a bonus, but a basic requirement. The discussion about sovereign cloud offerings also makes it clear that data control will become a strategic must in 2025.

Companies are focusing on the public cloud in the long term

The public cloud is establishing itself as a target platform. Currently, 42% of companies use the public cloud predominantly or exclusively. And even though 39% currently r e l y on balanced hybrid models, i.e. the balanced use of public and private clouds, the path is clear for many public cloud users: by 2028, 65% want to run more than half of their productive applications in the public cloud. Cloud-first is clearly at the top of the cloud strategies with 62%. At the same time, the vast majority of companies are pursuing a multi-cloud approach. This allows them to exploit scalability and innovation potential while a v o i d i n g technological dependencies. Sovereign cloud offerings strengthen trust in the public cloud and make it easier to meet regulatory requirements.

Budget considerations in the context of increased sovereignty

Sovereignty and data sovereignty are also reflected in companies' financial planning. For example, 44 percent of companies indicate a willingness to pay up to a fifth more. According to the survey, one in ten companies would even consider a surcharge of over 30 percent. These figures show that companies are focusing on sovereignty. However, the extent to which this willingness to pay is reflected in real additional expenditure remains to be evaluated.

Financial Operations (FinOps) as a strategic advantage

The cloud is losing some of its role as the primary cost reducer. While 67% still noticed significant cost reductions through cloud use in 2024, the figure was 61% in 2025. The trend clearly shows that strategic FinOps management is needed. A mature FinOps framework ensures transparency about consumption, links budgeting with technology and distributes responsibility along the entire development and operating cycle. The ability to continuously correlate costs and benefits is thus becoming a decisive competitive factor. Cost efficiency is not automatically achieved through cloud migrations, but through continuous optimization and the close integration of finance and technology teams.

A holistic approach to security

By 2025, cloud security will no longer be a purely technical issue and will continue to establish itself as a company-wide mandatory exercise. The imminent transposition of the NIS2 Directive into German law at the beginning of 2026 will noticeably increase the pressure to catch up with European pioneers. At the same time, an increasingly holistic approach to security is becoming apparent. When it comes to security measures, companies are shifting their focus from selective defense to proactive measures such as permanent monitoring. Zero-trust concepts and associated services are becoming the new normal. Security incidents are seen as a given and companies are preparing accordingly.

Artificial intelligence (AI) as a cloud-based value creation opportunity

The companies surveyed are increasingly hosting their analytics solutions in the cloud, while on-premise environments are becoming less important. The analytics solutions are most frequently hosted in hyperscaler clouds. In addition
92 percent of the companies surveyed use large language models (LLMs) to analyze and summarize unstructured data. analyze and summarize unstructured data. Generative AI is currently dominated by end-user tools that increase personal productivity. In addition, the first companies are using AI-based performance and compliance monitoring, which can detect risks at an early stage, particularly at the interface between man and machine.

We want to provide guidance with the Cloud Monitor 2025. Where do German companies stand today? What obstacles are slowing them down, what recipes for success are working? We invite you to use the findings as an impetus for your own roadmap.

Should you encounter any uncertainties or have new ideas for questions, please feel free to contact us. We look forward to your feedback and a lively exchange and wish you an insightful read.

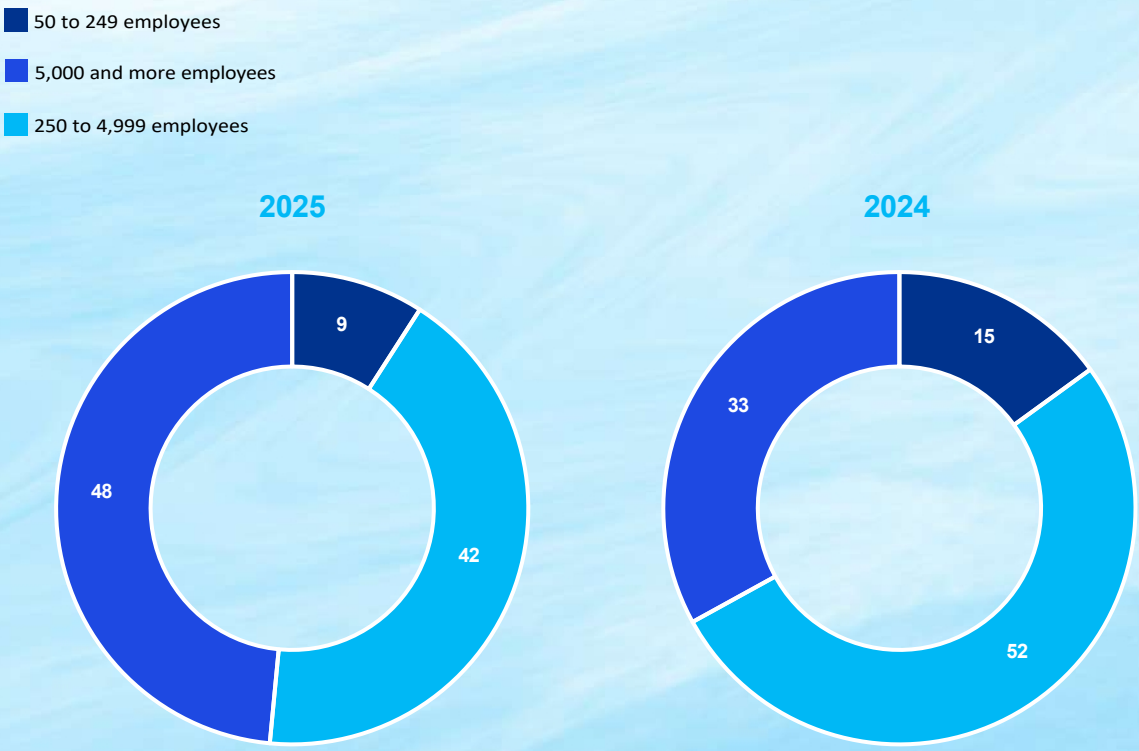
We would also like to draw your attention to the following: In addition to the Cloud Monitor 2025, KPMG Germany will also be publishing a decoupling of Financial Services in October.

Methodology

The Cloud Monitor is a company survey that has been conducted annually since 2012. The data basis for this year's Cloud Monitor was collected via computer-assisted web interviews (CAWI) in June 2025. The Cloud Monitor 2025 focuses on the general use of cloud computing, public cloud computing, cloud security, AI and data as well as FinOps and cost management. ESG aspects of cloud use are also once again included in the study results. New additions this year: budget considerations on the topic of sovereign cloud.

The sample size for the Cloud Monitor 2025 comprises 509 German companies with at least 50 employees. The respondents are managers from the following departments: Engineering, DevOps or IT/OT Operations, FinOps or IT/OT Operations.
cloud financial management, digitalization/innovation, finance or IT controlling or procurement, as well as members of management or the Executive Board. The target group was selected in such a way that companies of different sizes and industries are sufficiently represented to make statistically reliable statements.

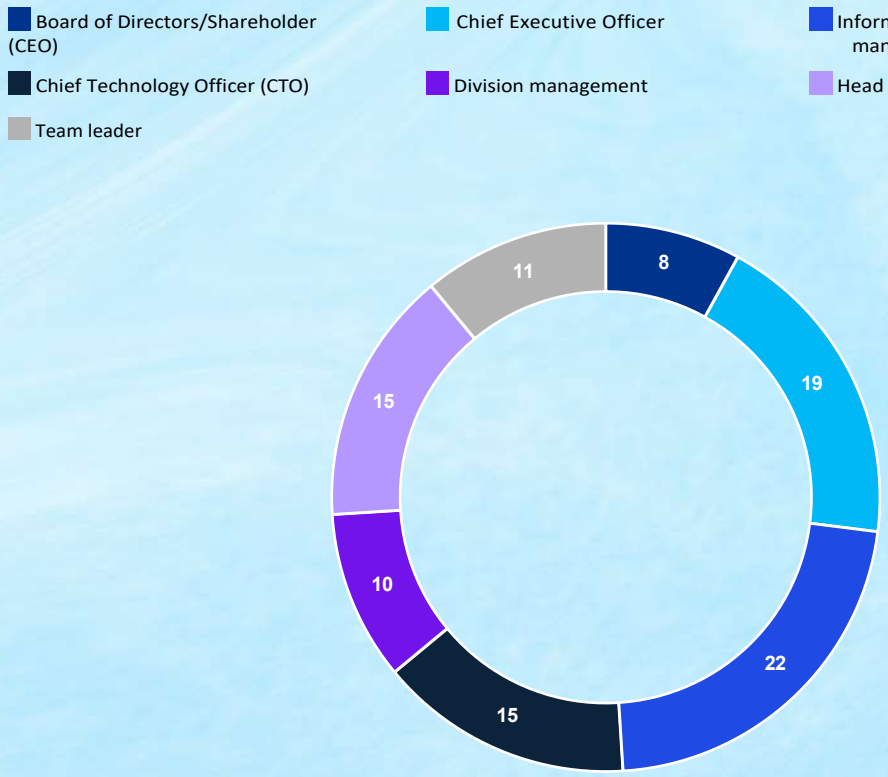
Figure 1:
Respondents by company size



Percentage of companies using cloud services; 2025: 509; 2024: n = 503 | Totals deviating from 100 percent are due to rounding differences
Source: KPMG in Germany, 2025

Figure 2:

Respondents by position



Percentage of companies that use cloud services, n = 509 Source: KPMG in Germany, 2025

The most important information at a glance - sorted by content

Use of cloud computing

42 %

of companies use mainly or only public cloud services, while 39% pursue a balanced hybrid approach. Only 19% use mostly or exclusively private cloud computing.

62 %

of companies pursue a cloud-first strategy.

58 %

of companies cite flexibility and scalability as an important cloud usage goal for the next five years - a jump from fourth place among the long-term goals last year to first place this year. In addition, 54% are aiming for increased IT security, which establishes security as a central, still relevant goal.

77 %

of the companies surveyed see cloud performance and stability as a must-have in 2025, seven percentage points more than in 2024. 58% see a sovereign cloud as a must-have.
Must-have, an increase of nine percentage points on the previous year. This shows that The demands on cloud providers are increasing.

Data and AI

96 %

of cloud-using companies obtain modern AI solutions from cloud providers. They host
AI solutions are most frequently hosted by hyperscalers. On-premise environments, on the other hand, are rapidly losing importance.

92 %

of companies use LLMs. This high adoption rate indicates that the survey provides a broad definition of "use" - from strategically implemented solutions to the use of LLMs by individual employees. The clear frontrunner is GPT from OpenAI with 61 percent usage and Google's Gemini model comes in second with 40 percent.

Cloud security

26 %

of companies state that they are well positioned for NIS2. The majority of companies still need to take action before the national NIS2 implementation comes into force at the beginning of 2026.

68 %

of companies continue to use traditional, password-based identity protection. A total of 61 percent also rely on multi-factor authentication.
companies combine modern procedures with traditional approaches without completely replacing them.

60 %

of companies rely on security monitoring as a measure against security incidents. A share of 58 percent carry out incident response exercises. Proactive monitoring complements a reactive approach and zero trust is being further expanded.

Public cloud - Computing

65 %

of the public cloud users surveyed plan to run more than half of their productive applications in the public cloud by 2028. This public cloud usage share currently stands at 39%.

FinOps and Cost management

98 %

i.e. the vast majority of companies, signal their willingness to pay a premium for a sovereign cloud. Specifically, 44% would accept a surcharge of up to 20% and 22% a surcharge of up to 10%. One in ten companies (ten percent) would even be prepared to invest more than 30 percent extra.

61 %

of the companies surveyed report rather or very large IT cost savings through cloud use.

Strategic imperatives in a connected cloud and AI world

Gernot Gutjahr
Partner, Consulting,
Head of Technology Strategy & Operations, Head of Managed Services,
KPMG AG Wirtschaftsprüfungsgesellschaft

The dynamics of technology and business are inextricably linked. Companies today are faced with the need to fundamentally re-evaluate their core strategies in the areas of artificial intelligence (AI), big data and cloud computing. We are witnessing a convergence of these disciplines that goes far beyond incremental improvements and is shaping the architecture of future business models.

The rise of the AI-first strategy as a business principle:
The integration of AI is no longer an optional technological add-on, but a central paradigm that is reshaping business strategy from the ground up. Companies that successfully implement AI position it at the center of their value chains - from product value chains - from product development to customer interaction and internal processes. It's about embedding data-driven intelligence into every facet of operations to achieve sustainable competitive advantage and enable continuous innovation. This requires a move away from pure technology implementation to a strategic AI enablement that encompasses culture, processes and capabilities.

Multi-cloud as a pragmatic necessity, not just an option:
The notion of a monolithic cloud strategy is giving way to the reality of a multi-cloud landscape.
Companies are increasingly leveraging the specific strengths of different cloud providers to ensure optimal performance, cost structures and resilience for different workloads. This strategy makes it possible to avoid lock-in effects and establish a "best-of-breed" architecture.
It is a development driven by the diversity of application landscapes and the need to meet specific latency, compliance or data processing requirements. However, managing this complexity requires robust orchestration and management tools.

Sovereign cloud in response to geopolitical realities and regulatory pressures:
The issue of data sovereignty and residency has evolved evolved from a niche consideration to a strategic imperative. In the face of increasing regulatory requirements and geopolitical tensions, organizations are being forced to implement solutions that ensure control over their data infrastructure. Sovereign cloud offerings - often in partnership with hyper-scalers or local providers - make it possible to leverage the benefits of the cloud while ensuring compliance with local laws and maintaining national or industry-specific data sovereignty. This is particularly relevant for critical infrastructures and sectors with sensitive data.

Interconnections and implications:
These three trends are deeply interconnected. A successful AI-first strategy is hardly conceivable without a robust multi-cloud infrastructure that offers the required scalability and flexibility for AI workloads. At the same time, the requirements

The choice of cloud providers and the architectures in a multi-cloud environment are significantly influenced by the requirements for sovereign clouds, especially when it comes to the provision of AI services that are trained or operated with sensitive data. The choice of cloud strategy must therefore take equal account of the company's AI ambitions and the regulatory framework. Only an integrated view of these elements will enable companies to successfully drive forward their digital transformation and create lasting value. The strategic imperative is not to manage these areas in isolation, but as parts of a coherent, future-oriented technology ecosystem.

01

Use of cloud computing

Cloud use is no longer just a technology issue, but has become the operational and strategic basis of digital business processes. In 2025, companies will continue to rely primarily on hybrid models with a clear focus on the public cloud. Cloud-first strategies are becoming more established and companies are using
multi-cloud strategies to combine different providers in a targeted manner. The cloud platform form enables flexible further development, rapid scaling and the implementation of regulatory requirements. In this context, agility is becoming a key long-term goal.
At the same time, awareness of digital sovereignty is growing: companies not only want to scale technologically, but also maintain control over data, infrastructure and compliance. Expectations of cloud providers are developing accordingly: performance, sovereignty and trust are no longer seen as a bonus, but as a basic requirement. Companies are in a phase of strategic consolidation. The cloud is acting as a dynamic driver of innovation.

1.1 Companies are focusing on hybrid formats with a clear public cloud trend

- 42% of companies use a public cloud environment for more than half of their cloud activities. Four percent have migrated completely to the public cloud and 38 percent tend to or predominantly use public cloud services.
- Private clouds are less important on the market. In total, only 19 percent prefer private cloud solutions.
- Just under two in five companies (39%) use both forms in roughly equal measure with a balanced hybrid approach.

The German cloud landscape in 2025 is nuanced. Companies are not looking for a dogmatic target architecture, but are consciously using several operating forms as they become more mature.
Overall, there is a clear trend towards the public cloud, albeit mostly in combination with private cloud models. So while the public cloud sets the direction, only very few companies (four percent) opt for a complete migration. Instead, they use a combination of public and private clouds to ensure scalability while maintaining data sovereignty. Sovereign clouds can bridge the gap between control and innovative strength.

Public cloud computing will be characterized by mixed model usage in 2025. In total, just under two in five companies (38%) tend to or predominantly use public cloud services. Around the same number of companies are not committed to either public or private clouds: almost two in five companies (39%) use public and private clouds in roughly equal measure with a balanced hybrid approach. This allows them to utilize the advantages of both models to the same extent and address scalability, flexibility and regulation at the same time.

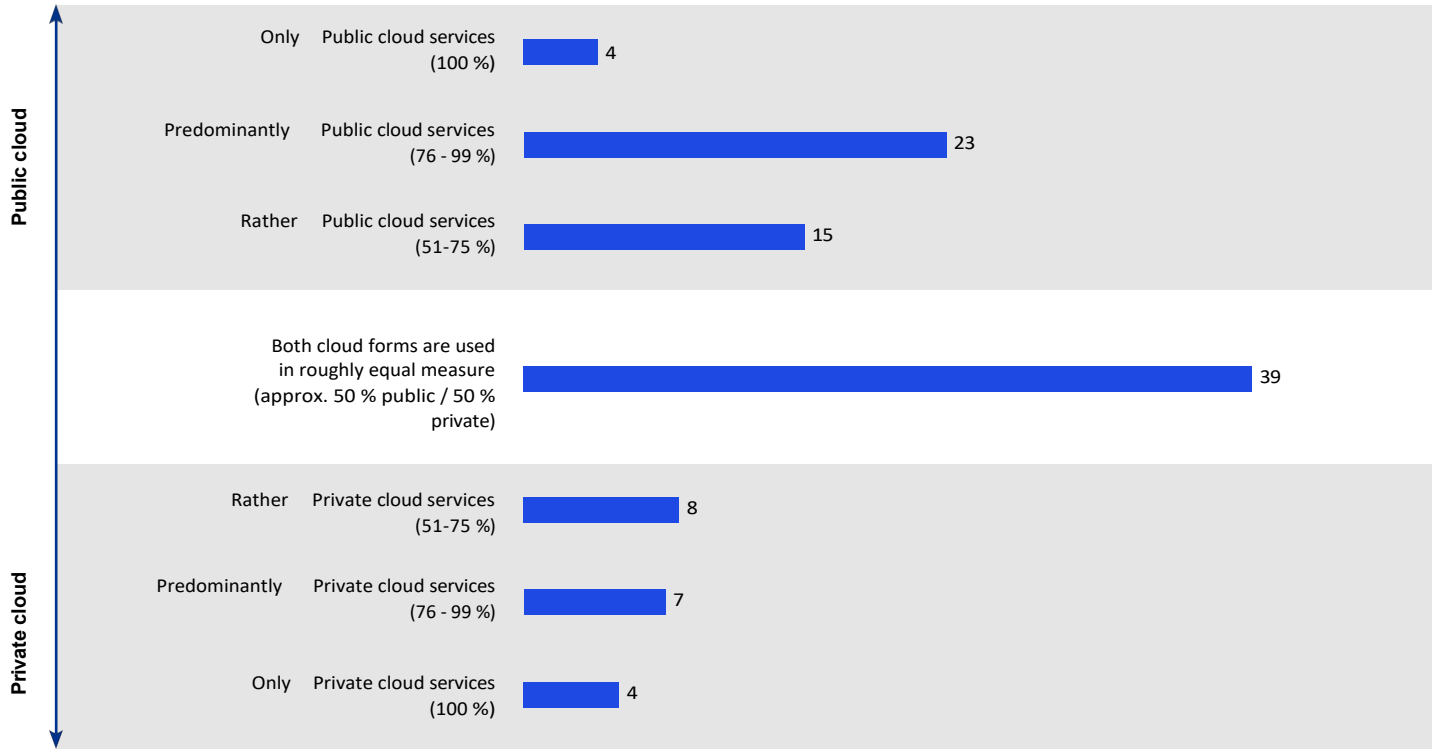
Private cloud models only play a subordinate role. Four percent use them exclusively and 15 percent tend to or predominantly use private cloud services. Taken together, this means that only 19% of the companies surveyed rely primarily on the private cloud. It may remain relevant for specific use cases involving sensitive data, but does not offer the same advantages as public clouds and is therefore losing relevance.

Companies therefore prefer public clouds, but are balancing security and scalability. Hybrid operating models with a clear tendency towards the public cloud provide the right basis for this. While companies continue to expand their use of the public cloud, they are also responding to acute compliance risks. New regulations such as the EU Data Act further increase the pressure to build cloud architectures that comply with regulations.

The Sovereign Cloud offering continues to shape the cloud debate, as the Sovereign Cloud can mitigate security concerns. Through improved control and data sovereignty, it increases trust and lowers inhibitions about using more data in the cloud. In this way, it can serve as a link between data protection requirements and the innovative power of large public cloud providers. Sovereignty is therefore becoming the next step in cloud usage. However, companies must also act in compliance with data protection regulations and keep an eye on economically viable infrastructure and cost factors. Cloud migration processes also take time. A clear roadmap is therefore necessary to ensure stable and secure cloud operations.

What form of cloud computing is currently used in your company?

Figure 3:
Proportion of cloud computing usage by cloud model



Percentage of companies using cloud services, n = 509 Source: KPMG in Germany, 2025

1.2 Cloud-first strategies remain leading and extend their lead

- 62% of companies are now pursuing a cloud-first approach. This is ten percentage points more than in the previous year.
- Cloud-only strategies are declining: from 23 percent in the previous year to 15 percent this year.
- Almost nine out of ten (87%) of the IT decision-makers surveyed orchestrate multiple providers and rely on a multi-cloud approach.

Companies will shift their cloud strategies even more towards cloud-first in 2025. Cloud usage will become a dynamic operating model and cloud users will adapt their strategies as required. Cloud technologies are increasingly forming the foundation of digital value creation, but companies prefer a balance of cloud and on-premise applications. Multi-cloud approaches remain at a high level and companies are managing their provider portfolio strategically.

Cloud-first has now firmly established itself as the preferred operating model. More than three out of five companies (62%) are pursuing this approach - a significant increase compared to the previous year (52 percent). After a brief decline in 2024, the cloud-first approach will regain importance in 2025 and further consolidate its leading position. The cloud therefore remains the preferred platform for applications, but without the compulsion to migrate completely.

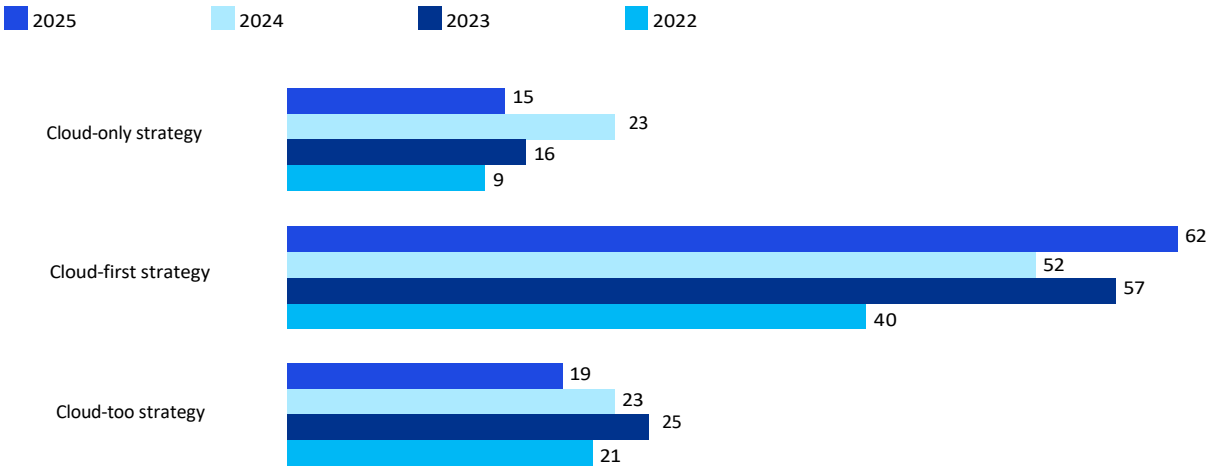
migration. At the same time, radical cloud-only strategies are losing some of their appeal. While 23% still relied on cloud-only in the previous year, this figure will only be 15% in 2025. Instead of relying entirely on cloud services and no longer operating their own servers or data centers, more companies are using a combination of cloud and on-premise solutions.
on-premise solutions.

Multi-cloud use is now established across all sectors. Of all companies surveyed, 87% are pursuing a declared multi-cloud strategy and are therefore relying on multiple providers to a similar extent as in the previous year. These strategies offer openness, scalability and access to different cloud environments. By combining different providers, companies can reduce dependencies, combine specialized services in a targeted manner and actively spread risks.

Flexible operating models are considered robust and companies do not rigidly pursue a cloud strategy. Instead, models are adapted and tailored to current needs and technical feasibility. This allows companies to mature their strategies. They are now aware that not every workload needs to be moved to the public cloud and that an individual review as part of a differentiated cloud strategy makes sense. The shift back from last year's cloud-only trend to cloud-first shows that instead of limiting themselves to the public cloud, companies are pursuing differentiated cloud strategies and prioritizing a pragmatic balance of workload, cost control and regulation.

Which of the following strategies is most likely to apply to your company's cloud transformation?

Figure 4:
Cloud transformation strategy over time



Percentage of companies using cloud services by survey year (2022/2023/2024/2025) n = 478/518/503/509 | Missing 100 percent = "No specific cloud transformation strategy.", "Other" or "Don't know."
Source: KPMG in Germany, 2025

1.3 Long-term cloud goals in terms of flexibility and scalability

- 58% of the companies surveyed named flexibility and scalability as the main long-term goal of cloud use for the next five years.
- Last year, this figure was only 45%. Since 2024, flexibility has thus moved up from fourth to first place among the long-term goals.
- 54% are also pursuing increased IT security. Security thus remains a central, still relevant goal.

Companies are rethinking their cloud goals for the long term. While cloud use used to be primarily security and cost-driven, the desire for agility, rapid scaling and adaptability is now coming to the fore. The cloud is increasingly seen as a driver of dynamic business models and its strategic added value lies in the flexibility it offers.

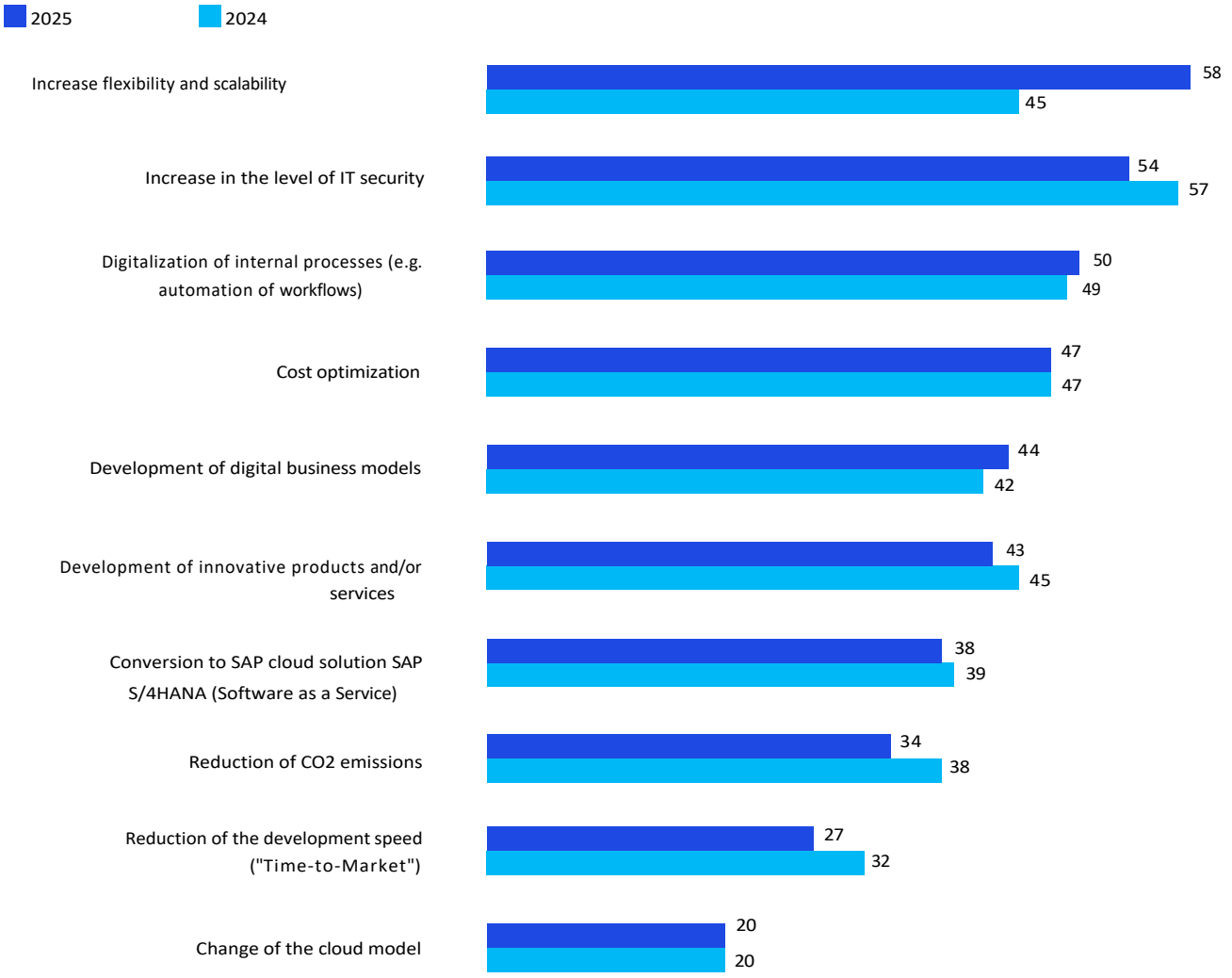
This is confirmed by the latest survey results. A share of 58% of respondents cite increased flexibility and scalability as the long-term goal of their cloud initiatives. This represents a significant increase of 13 percentage points compared to 2024 (45%). This means that agility has moved from fourth place to the top of the list of long-term cloud goals within the space of a year.

Alongside the pursuit of agility, the cloud remains a key element for central corporate priorities. Increased IT security comes in second place and thus remains a key cloud usage goal.
At 54%, IT security as a goal is at a comparable level to the previous year. Cloud security therefore remains important, but is increasingly seen as a basic requirement and no longer a primary objective, as companies are expanding their security strategies holistically (see section 3.3) and are more resilient. A total of 47% also continue to cite cost optimization as a long-term goal of cloud use. As the initial savings effects of cloud use are currently somewhat relativized
(see section 4.1), this value remains unchanged compared to the previous year. Reduced costs are not gaining in strategic importance.

This focus on agility is shifting the role of the cloud from an IT infrastructure issue to a driver of innovation.
Companies are increasingly seeing it as a platform for the development, testing and iterative improvement of new products, services and business models. A step-by-step approach is recommended: first experiment, then scale. However, more than just technological infrastructure is needed to sustainably drive growth in the cloud. Instead, the focus is on the continuous development of skills and processes, which must be considered on an interdisciplinary and organization-wide basis.

What goals is your company pursuing with its cloud strategy over the next five years?

Figure 5:
Cloud strategy goals in companies in a year-on-year comparison



Percentage of companies pursuing a cloud transformation strategy, by survey year (2024/2025) n = 499/491 | Multiple answers possible.
Source: KPMG in Germany, 2025

1.4 High-performance clouds will be a basic requirement in 2025

- In 2025, a powerful and stable cloud will be a basic requirement for 77% of the companies surveyed - seven percentage points more than in the previous year.
- A total of 72% consider the security and compliance of their cloud provider to be essential.
- A sovereign cloud is a must-have for 58 percent. This corresponds to an increase of nine percentage points compared to the previous year.

The performance and stability of the cloud is at the top of companies' expectations of cloud providers. This is a must-have for 77% of respondents, seven percentage points more than in the previous year. This means that high-performance clouds have developed from an important plus point to an indispensable basic criterion. The digital maturity of companies is growing, as is the complexity of applications, and cloud providers must keep pace with this in terms of technology and infrastructure.

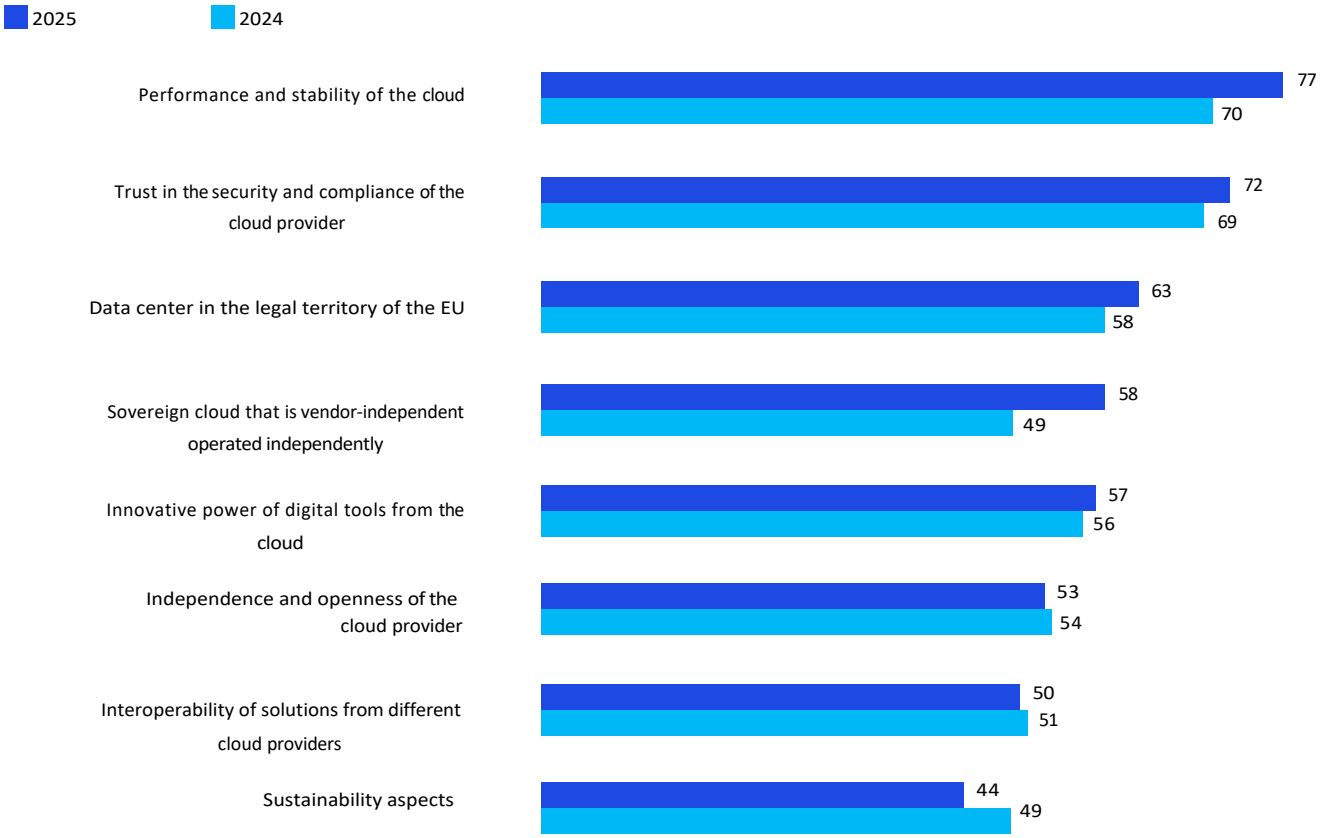
However, companies are demanding more from their cloud providers than just technical performance. Due to growing security awareness on the part of companies and increasingly complex regulatory requirements (see section 3.1), trust is becoming a key prerequisite for any cloud usage. The security and compliance of their providers are a must-have for 72% of the companies surveyed. Without credible security concepts and reporting, providers quickly lose acceptance.

Regulatory and political framework conditions are increasing the focus on control over data. A sovereign cloud is indispensable for 58%, a significant increase compared to 2024
(49 percent). In the context of increasingly relevant data protection considerations, the sovereign cloud is becoming a strategic must for many companies. Heavily regulated industries and companies with sensitive data in particular are raising their awareness of digital sovereignty.

In order to meet the increased expectations of performance, security and sovereignty, companies should view their relationship with the cloud provider as a partnership-based quality alliance, including transparent service agreements, written security concepts and comprehensible roadmaps. Building on this, measures such as multi-cloud approaches, regular security audits and compliance checks unfold their full value for company-wide digital resilience.

How important are the following criteria and services for your company when selecting a cloud provider?

Figure 6:
Requirements for cloud providers in a year-on-year comparison



Percentage of companies that use cloud services and describe the respective aspect as a "must-have", n = 509 Source: KPMG in Germany, 2025

1.5 Cloud use can help with ESG reporting support

- Almost seven out of ten companies (69%) rate ESG criteria as (very) important in their cloud strategy.
- In the previous year, however, this figure was 77%. Compared to 2024, the relevance has therefore fallen by eight percentage points.
- Companies with cloud-only strategies prioritize ESG the most. Here, 82% consider ESG to be important or very important. For companies with cloud-first strategies, the figure is 71 percent, and 61 percent for cloud-too strategies.

Despite a slight decline, ESG will remain a central strategic guideline in 2025. Of the companies surveyed, 69% consider ESG to be relevant in their cloud use. This sends a clear signal that ESG is not a short-lived trend, but has become an integral part of long-term cloud planning.

However, companies are showing increasingly pragmatic expectations of their cloud providers and ESG aspects. In the previous year, 77% of the companies surveyed rated ESG as (very) important.
This reflects the cost pressure resulting from the economic situation, which is causing ESG to take a back seat for some companies.

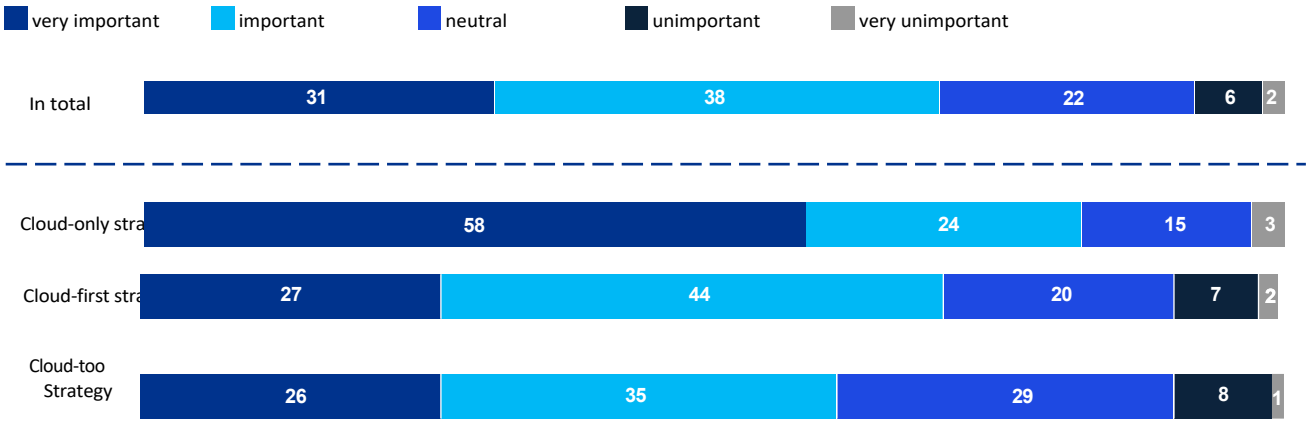
However, there are still fundamental connections between ESG and cloud use. ESG can be a decisive cloud migration argument, as companies can outsource their scope emissions in the public cloud.
2- emissions in the public cloud. Cloud-native platforms provide standardized tools and processes that facilitate ESG reporting. Thanks to the tools available, public cloud models also serve as a lever for scalable reporting.

The more consistently companies move to the cloud, the more firmly they embed ESG in their strategy. Companies with cloud-only strategies (82%) have higher ESG approval ratings than those with cloud-first (71%) or cloud-too strategies (61%). This difference can be explained by both internal company factors and characteristics of the cloud infrastructure. Companies with cloud-only strategies demonstrate a high level of digital maturity and therefore possibly also use the scalability of cloud providers more frequently for ESG data collection and reporting.

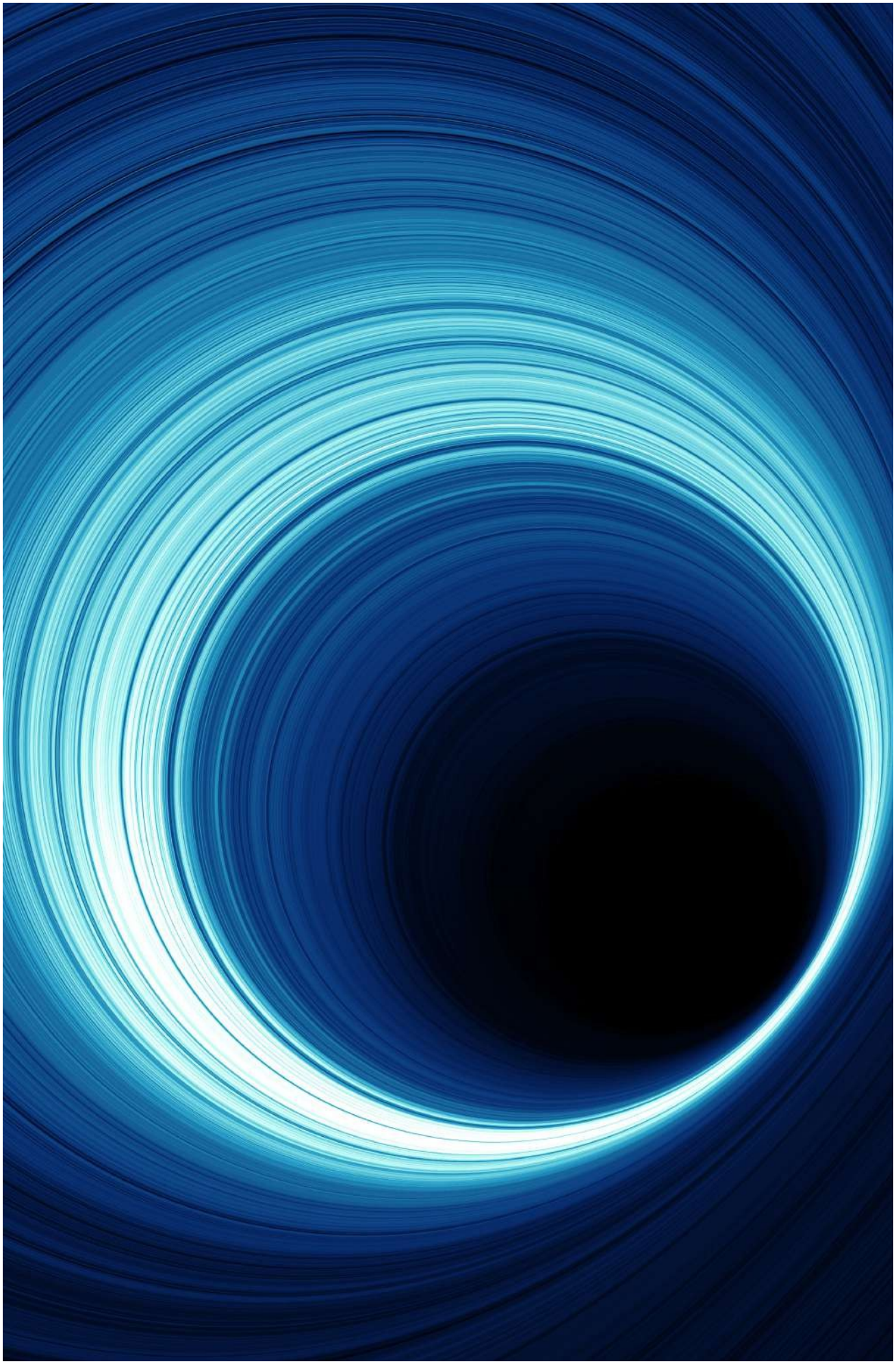
ESG therefore remains an integral part of the cloud strategy for many companies, as cloud solutions offer significant leverage for more sustainable IT through optimized energy and resource usage as well as transparency in the supply chain. At the same time, ESG is now competing more strongly with other priorities such as cost optimization or security. Nevertheless, ESG aspects remain a central point of orientation for the majority of companies. By following this, they combine economic efficiency with responsibility and create sustainable competitive advantages.

How important are ESG aspects in your company in the context of cloud use?

Figure 7:
Relevance of ESG aspects in the context of cloud use according to cloud strategy



Percentage of companies using cloud services, n = 509, by cloud strategy n = 78/318/95 | Totals differing from 100 percent due to rounding differences.
Source: KPMG in Germany, 2025



The potential of community and edge cloud: rethinking decentralized intelligence

Vojislav Kosanovic,
Partner, Consulting,
Technology Strategy & Operations,
KPMG AG Wirtschaftsprüfungsgesellschaft

The data processing landscape is subject to continuous evolution. While the public cloud remains a central pillar of IT infrastructure, specialized architectures such as the community cloud and edge computing are becoming increasingly important. They address specific requirements for data processing, security, latency and collaboration, which are becoming increasingly critical in the era of networking.

Edge computing as a catalyst for real-time innovation:
Moving data processing to the edge of the network, closer to the data source, is not just a technical optimization, but an enabler for new business models and operational efficiencies.
Industries from manufacturing (Industry 4.0) to retail and autonomous driving benefit from low latency and the ability to analyze and respond to data in real time. Edge computing makes it possible to make decisions locally and immediately without having to rely on the central cloud. This is crucial for applications that require maximum reliability and minimal delays and paves the way for smarter, more autonomous systems.

Community clouds to promote industry-specific ecosystems and strengthen sovereignty:
Beyond the individual cloud strategies of companies, community clouds are increasingly emerging. These are often industry- or domain-specific and enable collaborative data processing and the exchange of information between participating organizations. The aim is to establish common standards, accelerate research and development projects or provide industry-wide services. Examples can be found in the healthcare sector (e.g. for the exchange of patient data under strict data protection regulations), in the regulatory environment (e.g. for the processing of sensitive data in accordance with VS-NfD), in defense (e.g. for the exchange of classified data or operations in the event of a crisis) or in the automotive industry (for shared test data of autonomous vehicles). These clouds create trusting environments for collaboration and leverage the potential of collective intelligence.

Decentralization in response to data volumes and latency requirements:
The exponential growth in the amount of data generated, particularly by IoT devices, and the need for real-time processing pose challenges for traditional cloud architectures. Decentralization through edge and community clouds is a strategic response to this. It reduces the need to transfer all data to a central data center, which saves bandwidth and drastically shortens latency times. This architecture is not only more efficient, but also more resilient to network outages and enables more robust data processing in critical environments.

Cross-connections and implications:
The community cloud and edge cloud are not isolated developments, but complementary extensions of the existing cloud landscape. Edge computing often generates and processes local data, which can then be aggregated, shared and analyzed via a community cloud or a central public cloud. For example, sensor data from machines could be pre-processed via edge nodes and made available anonymously via an industry-specific community cloud for benchmarking or joint AI model development. These synergies create new opportunities for data-driven innovation and more efficient processes by combining the strengths of decentralization with those of collaboration. The strategic challenge is to intelligently integrate these specialized cloud models into the overall cloud strategy, taking into account the complex security, governance and data management requirements. It is about finding the right balance between centralized control and decentralized autonomy in order to leverage the full potential of these architectures.

02

Public cloud computing

The public cloud is becoming a strategic target platform. More and more public cloud users are moving productive workloads to the public cloud in order to take advantage of scalability and innovation potential. However, this transition is taking place in small, planned steps. Public cloud users have ambitious goals for the coming years. However, historically grown IT structures, organizational processes and personnel bottlenecks are setting the pace and slowing down the public cloud migration. Strategic change management and differentiated migration paths are crucial to minimize risks. The public cloud transformation requires time, trust and a profound restructuring of historically grown IT architectures. If existing systems, governance and cross-team competencies are synchronized, the opportunities of the public cloud can be fully exploited. public cloud can be fully exploited.

2.1 Increasing public cloud workloads and ambitious goals

- In 2025, 39% of public cloud users will already be hosting more than half of their productive workloads in the public cloud - three percentage points more than in 2024.
- The target picture for the coming years is clear: by 2028, 65% of the public cloud users surveyed plan to run more than half of their productive applications in the public cloud.
- This contrasts with today's reality. Currently, 60 percent of public cloud users still operate more than half of their workloads outside the public cloud.

More and more public cloud users are increasingly moving productive applications to the public cloud. However, the change remains deliberately gradual. Public cloud users are focusing on controlled, maturity-driven growth: they are increasing the public cloud share in a targeted manner, but still need to adapt their ambitious plans to the existing IT reality.

In 2025, a total of
39% of public cloud users will run more than half of their productive applications in the public cloud, which corresponds to a moderate increase of three percentage points compared to the previous year. This rather cautiously growing share reveals cautious strategies. Public cloud users are gradually relocating applications and workloads in order to keep risks and migration costs manageable.

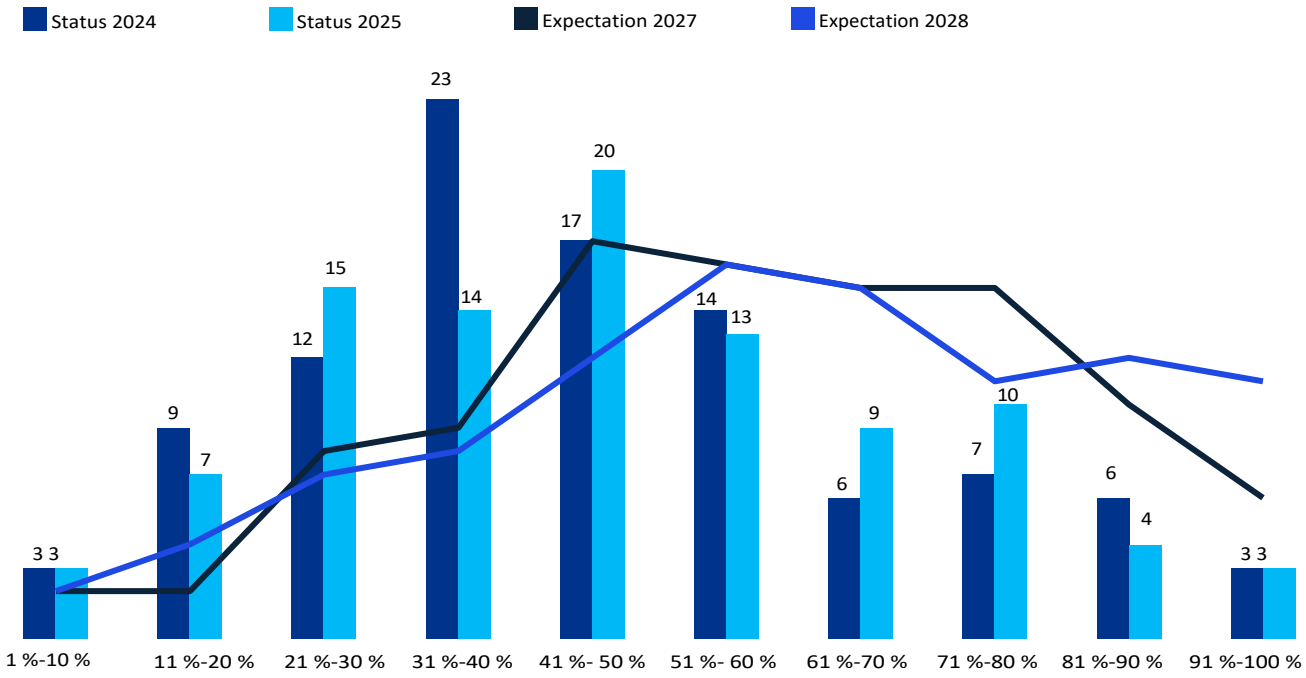
At the same time, the growth forecast shows a clear path: In three years, 65 percent of public cloud users want to run over half of their productive workloads in the public cloud. The public cloud is clearly positioning itself as a target platform and the proportion of applications running in the public cloud will increase significantly by 2028.

Despite their ambitious goals, public cloud users still have a considerable migration path ahead of them. A total of 60 percent of them still run half or less of their productive applications in the public cloud. There is a clear gap between the target image and the current status and public cloud users continue to rely on a hybrid approach, but are aiming for a higher public cloud share. Some of them are still in the process of establishing stable architectures and building trust in cloud technologies.

A sustainable migration in which the benefits of the public cloud are fully utilized is associated with considerable time expenditure and the conversion of existing IT structures. The migration of sensitive sensitive data and processes requires patience and trust in robust security and governance concepts. Agile change management accelerates the transition and at the same time ensures the ability of companies using the public cloud to act.

What percentage of productive applications in your company do you currently run from the public cloud and what percentage do you expect to run from the public cloud in three years' time?

Figure 8:
Current and expected share of productive applications in public clouds



Percentage of companies that use public cloud services, by survey year (2024/2025) n = 388/490 | Missing 100 percent = "0 %" or "Don't know."
Source: KPMG in Germany, 2025

2.2 Structural hurdles are slowing down public cloud migration

- According to the survey, 45% of the public cloud users surveyed cited the modernization of the existing IT landscape as a challenge. This puts it in first place.
- For 41 percent of public cloud users, adapting internal processes is a major organizational hurdle.
- Large companies using the public cloud are almost twice as likely to struggle with finding specialists (40 percent) as public cloud users with 50 to 249 employees (21 percent).

The increasing migration to the public cloud brings with it challenges that are often rooted in internal company structures. The biggest obstacles lie less in the public cloud itself than in historically grown infrastructures.

The most common difficulty in integrating public clouds is adapting the internal IT infrastructure (45%). The most urgent bottleneck therefore lies in outdated structures and legacy systems of public cloud users. There is often a lack of interfaces, process maturity or resources to seamlessly integrate cloud services into existing IT systems.
At the same time, it is essential for public cloud users to adapt these infrastructures in order to remain technologically competitive and avoid problems later on.

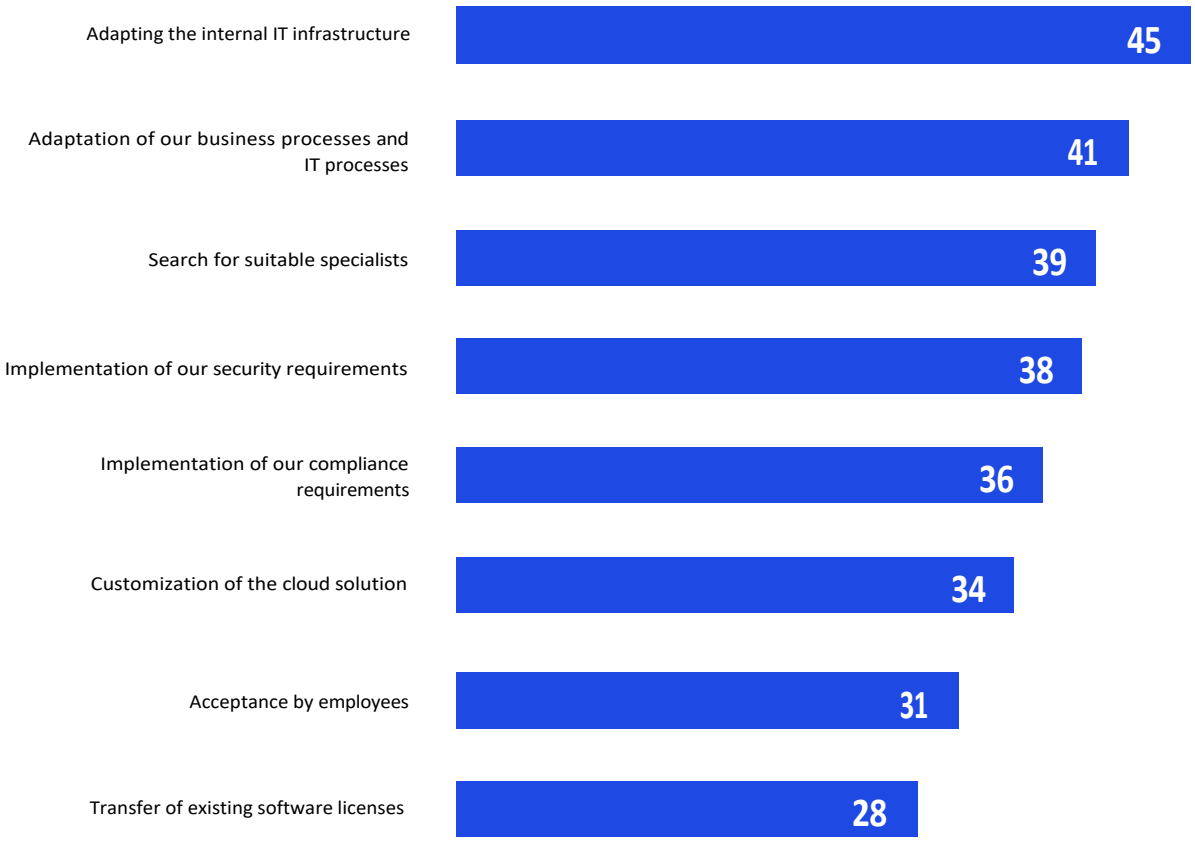
Adapting processes is also a challenge for a good two in five public cloud users (41%). This makes it clear once again that organizational and personnel factors are slowing down public cloud integration. It is not only slowed down by technology, but also by corporate aspects. Hurdles in the implementation of security requirements (38%) further highlight IT infrastructural deficits.

The search for specialists reveals further weaknesses at company level and is a key factor for 39% of the public cloud users surveyed. This skills gap poses challenges for larger organizations more often than smaller ones. While only 21 percent of public cloud-using companies with 50 to 249 employees are affected, the proportion is 42 percent for companies with 250 to 4,999 employees and 40 percent in large public cloud-using companies (5,000 and more employees). This once again highlights the weak point of outdated infrastructures: larger and therefore often older companies often have more complex structures and change management also becomes a challenge at personnel level.

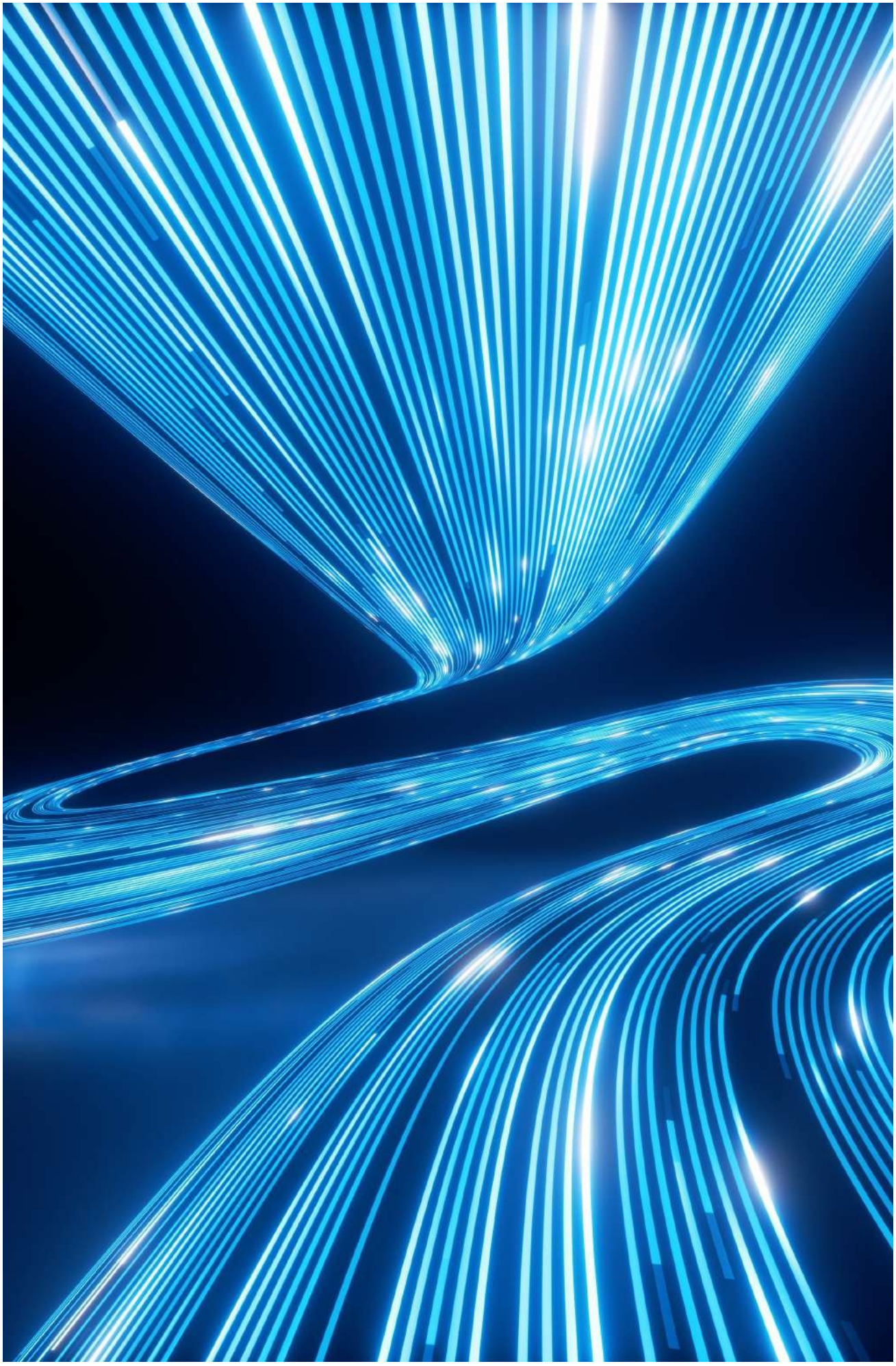
Clear milestones and roadmaps help with the migration to the public cloud. Deliberately migrating related applications in "move groups" is one measure to avoid fragmentation. The 6R strategy of cloud migration - Rehost, Replatform, Repurchase, Refactor, Retire and Retain - gives public cloud users a clear roadmap for applications of varying maturity. Costs, risks, agility and innovation potential can be strategically balanced, from a quick "lift and shift" to phased modernization to the decommissioning or targeted retention of individual workloads. A generic approach falls short of the mark. Instead, individual solutions tailored to the industry and company size are needed.

What difficulties did your company face in 2024 when integrating the public cloud solutions it uses into its existing IT infrastructure?

Figure 9:
Difficulties with the integration of public cloud solutions



Percentage of companies that use public cloud services, n = 490 | Multiple answers possible. Source: KPMG in Germany, 2025



Public cloud computing: the indispensable basis for digital transformation

Christian Decker
Partner, Consulting,
Technology Strategy & Operations
KPMG AG Wirtschaftsprüfungsgesellschaft

The public cloud has evolved from a novel option to an indispensable pillar of enterprise IT. Its ability to offer unprecedented scalability, flexibility and access to innovative services has made it the preferred foundation for digital transformation. But simply using it is no longer enough; the focus is shifting to strategic optimization and value creation from this essential resource.

Public cloud as the standard for new developments and modernization:
The public cloud is now the de facto standard for developing new applications ("cloud-native") and modernizing existing IT infrastructures. Companies are recognizing that the agility offered by cloud services such as containers, serverless computing and managed databases is critical to responding quickly to market changes and delivering innovative products and services. The speed of innovation in hyperscalers exceeds the capabilities of most on-premise environments, making the public cloud the first choice for future-oriented architectures.

Optimizing cloud usage through automation and intelligent control: With increasing public cloud adoption, efficient usage is coming to the fore. It is no longer
It is no longer just about migration, but about the continuous optimization of performance, availability and costs. This is driven by the use of automation tools, infrastructure-as-code practices and intelligent management platforms. These enable the dynamic adjustment of resources to actual requirements, the automation of provisioning and maintenance and the identification of optimization potential. Manual management of complex cloud environments is no longer practicable in the face of scaling.

The expansion of the cloud ecosystem as a driver of innovation:
The major public cloud providers are not just infrastructure suppliers, but have built up comprehensive ecosystems of services, tools and partners. These range from highly specialized AI and machine learning services to IoT platforms and industry-specific solutions. Companies that make strategic use of these ecosystems can accelerate innovation cycles and rely on established, scalable services instead of having to develop everything themselves. The ability to select and integrate from this rich pool is a decisive competitive advantage.

Cross-connections and implications:
The public cloud provides the scalable and flexible foundation for almost all digital initiatives. An effective FinOps strategy is essential to make costs transparent and controllable in the public cloud, while cloud security directly benefits from and extends the native security capabilities of public cloud providers. Without the elastic infrastructure of the public cloud, scaling AI and big data workloads would be difficult to realize. The public cloud also enables companies to accelerate their AI strategies through access to powerful computing resources and pre-built AI services. It is therefore crucial to view the public cloud not as a mere cost factor, but as a strategic enabler whose potential is maximized through intelligent management approaches, security strategies and a clear FinOps culture. The future of corporate IT is inextricably linked to the strategic and optimized use of the public cloud.

03

Cloud-Security

In 2025, cloud security will not be determined by technical measures alone. Data protection, governance and compliance will continue to take center stage and will be integrated into existing business processes. The national implementation of the NIS2 directive will create a binding framework that will significantly increase the pressure on companies to act. The first companies are adjusting their processes, even if there are still noticeable gaps. A two-pronged approach dominates identity protection and companies are focusing on gradual modernization. They are protecting existing legacy systems and integrating modern, cloud-based processes at the same time. At the same time, the maturity level of the company's internal IT is increasing, enabling the further development of security strategies. The focus is shifting from selective protection measures to continuous monitoring. Zero-trust models are becoming increasingly sophisticated and a security mentality is gaining ground that does not rule out potential security incidents, but proactively anticipates them. Monitoring, regular incident response tests and multi-layered defense mechanisms form the foundation of a modern cloud security architecture. If you want to guarantee security, you need a holistic strategy that combines data protection, regulatory requirements and operational security in a resilient overall architecture.

3.1 Cloud security between data protection, Compliance and regulation

- Cloud security goes hand in hand with various challenges. Data protection (46%) and compliance (39%) top the list.
- A good half of companies that tend to or predominantly use private cloud (51%) and companies with balanced hybrid models (50 percent) see data protection as a challenge. This contrasts with only 39% of companies t h a t tend to or predominantly use public clouds.
- More companies consider themselves ready for NIS2 than in the previous year: 26% feel they are well prepared (2024: 22%).

Today, cloud security is primarily an organizational and compliance-driven challenge. Data protection, governance and compliance have a deep impact on corporate structures and require close integration with operational processes. At the same time, regulatory pressure is increasing.

With the planned transposition of the NIS2 directive into German law at the beginning of 2026, the pressure on companies to act is already increasing. The first companies are actively preparing for the upcoming regulatory requirements and adapting their security strategy accordingly. Current survey results confirm this: This year, more companies than last year state that they are well prepared for NIS2. Around a quarter (26%) believe they are well prepared - an increase compared to 2024, when just over a fifth (22%) shared this view. However, caution is still required. Because even if some companies see themselves as better positioned, all companies will ultimately have to follow suit. The European comparison shows that countries such as Belgium are lagging behind in the implementation of NIS2

are already significantly more advanced. Germany must therefore take targeted measures to catch up in terms of regulation and organization.

At 39 percent, compliance ranks second among the cloud security challenges to be mastered.
Regulatory frameworks, the establishment of control mechanisms such as NIS2 and complex laws lead to uncertainty among companies. Parallel regulations such as the EU AI Act add to the complexity.

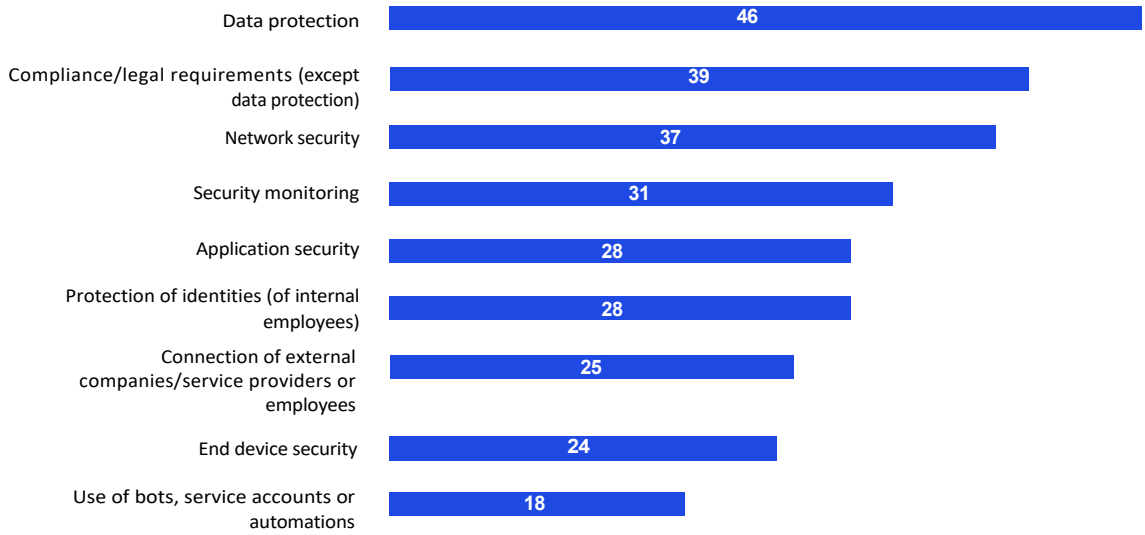
Companies are increasingly confronted with structural challenges in the area of cloud security. Data protection in particular is perceived as a critical factor - a total of 46% of the companies surveyed classify it as a key security challenge. The choice of cloud model influences the perception: 51% of companies that tend to or predominantly use private cloud services and 50% of companies with balanced hybrid models see data protection as a challenge. This contrasts with only 39% of respondents who tend to or predominantly use public clouds.

Regulatory requirements also vary depending on the sector. While some sectors are confronted with fewer requirements, others have to pay more attention to data sovereignty and control mechanisms. These differences require individual security concepts that take both technical and organizational aspects into account.

Companies are increasingly closing existing gaps, but must consistently integrate data protection, regulatory requirements and governance into their structures. For a long-term, resilient security architecture, it is advisable to establish a comprehensive compliance strategy at an early stage.
Clearly defined governance makes cloud strategies and responsibilities transparent. This enables companies to adapt their organizational processes to new legal and security-related requirements in a targeted manner - a decisive step towards greater resilience and future viability.

What are currently your three biggest security challenges when using cloud solutions?

Figure 10:
Security challenges



Percentage of companies that use cloud services, n = 509 | Multiple answers possible (max. 3 answers). Source: KPMG in Germany, 2025

3.2 Identity management is becoming more secure. Companies are gradually introducing modern procedures

- With 68 percent usage, classic password-based identification protection is the number one method used.
- A good three out of five companies (61 percent) use multi-factor authentication.
- Identity-as-a-Service (IDaaS) is proving to have a promising future. Current use (44 percent) and future planning (42 percent) are almost on a par.

When it comes to protecting digital identities, companies rely on a combination of traditional and modern methods. Instead of radical breaks, modern identity protection is undergoing gradual further development and traditional password-based authentication remains dominant. More modern procedures complement it, but have not yet replaced it. The long-term goal is holistic, networked identity management instead of isolated individual solutions.
Cloud-based service models standardize identity processes company-wide.

Traditional passwords remain the dominant method of identity protection: the survey shows that 68% of all companies surveyed use authentication in this way. In addition to this classic method, more modern alternatives increase company-wide identity security. With 61% usage, multi-factor authentication (MFA) has established itself as a further standard.

A good half of the companies surveyed also use cloud single sign-ons (SSOs) (53%) and passwordless authentication such as passkeys or biometric procedures (51%). Both methods are now regarded as modern additions, but more as additive elements within flexible strategies, not as a complete replacement for more traditional methods.

Service models such as Identity-as-a-Service (IDaaS) are seen as trend-setting. IDaaS is planned by almost as many companies surveyed (42 percent) as are already using it (44 percent). This trend promises scalable and future-proof identity management in the cloud.

Companies tend to use modern security measures as a supplement and avoid a fundamental renewal of their identity protection. The reason for this is existing legacy systems, which make the technological implementation of modern identity protection methods more difficult. Modernized security must be compatible with technological feasibility.

Sustainable change is therefore achieved through gradual integration instead of abruptly replacing existing procedures. The aim should be to secure existing procedures and not to replace them hastily. In addition, the underlying IT architectures must be renewed in order to guarantee the ability to act. Those who understand identity management as a strategic platform and end-to-end service model are secure in the long term.

A clear roadmap is recommended for companies introducing or expanding IDaaS platforms: First, a target picture for identity governance should be defined that takes into account existing IAM structures, regulatory requirements such as NIS2 and eIDAS 2.0 as well as company-specific role models.

Building on this, central use cases such as onboarding, role assignment and external identities must be prioritized. The choice of platform must not only meet functional requirements, but also enable smooth integration into existing ERP, HR and GRC systems. The introduction ideally takes place ideally via pilot areas, flanked by a central competence team for identity management. This creates a scalable governance structure that combines regulatory security with operational efficiency and establishes identity management as the strategic backbone of modern cloud security.

Which of the following measures is your company taking to modernize identity protection?

Figure 11:
Measures to modernize identity protection

Percentage of companies that use cloud services, n = 509 | Totals deviating from 100 percent are due to rounding differences.
Source: KPMG in Germany, 2025

3.3 In 2025, companies will focus on security monitoring

- This year, security monitoring is the number one measure for security incidents (60%). This shows a clear increase compared to the previous year.
- Incident response exercises follow in second place with 58 percent.
- Zero Trust strategies are becoming increasingly sophisticated. Companies are using all services as part of zero trust more frequently than in the previous year - with network security leading the way (69%).

With increasing cloud usage, the need for integrated and holistic security solutions that cover all levels of the IT infrastructure is growing.
Companies are therefore combining proactive and reactive security strategies for maximum resilience.
The use of available services is also increasing with zero-trust concepts. Companies are using new security technologies in a targeted manner and are open to innovative approaches.

In 2025, companies will shift their focus when it comes to measures against security incidents. Security monitoring is in first place with 60 percent; in 2024 it was still in third place. Incident response exercises follow in second place with 58% and hardly any change compared to the previous year. This underlines the shift towards continuous, proactive monitoring. Reactive measures are therefore not being significantly expanded, but remain relevant. This combination of proactive and reactive measures strengthens the resilience of security processes.

Zero Trust is becoming the cornerstone of modern cloud security. Companies are using all services more extensively than in the previous year. The focus is on network security (69% use, up four percentage points on 2024) and security monitoring (64%, up eight percentage points on 2024). To protect sensitive information, 63% use data protection (four percentage points more than in 2024), while 56% rely on identity protection for identity-based access control (eight percentage points more than in 2024). These results show: Companies' zero-trust strategy is based on graduated, interlocking layers of protection. The result is a multi-layered defense for identities, data, applications and networks.

In 2025, zero trust is not an entirely new topic, but it is experiencing a new dynamic, made possible by the growing maturity of companies and modern technologies. This means that companies can now implement zero trust with increasing consistency. It is crucial to establish Zero Trust as a binding framework and to combine technologies with expertise.

To ensure that Zero Trust works not just as a technical concept, but as an end-to-end security principle, companies must consistently integrate it into their cloud usage. Consistent implementation is possible if all relevant cloud services - from network access to identity and data controls through to application security - are placed under uniform guidelines and monitoring mechanisms. Measurable progress can be recorded using specific KPIs - for example, how many systems are protected by identity-based access controls, how quickly security-related incidents are responded to, how regularly incident response tests are successfully carried out or how many rule violations are automatically detected and documented. Companies that systematically record and evaluate such KPIs create

transparency and can further develop their zero trust strategy in a targeted manner. Those who not only use zero trust selectively, but also systematically operationalize it across all cloud levels, create a resilient basis for preventive security and regulatory traceability.

In 2025, companies are increasingly pursuing an "assume-breach" mentality in their security strategies. In 2024, cloud outages of large hyperscalers increased by increased by almost a fifth[1]. The possibility of a security incident must now be considered a given and a robust security architecture is becoming a business-critical requirement. To take cloud security to the next level, organizations must now consider security as an integral part of all layers, from identities to data to applications. Security is becoming a cross-sectional task and DevOps and specialist departments also bear responsibility.

Cloud security: from brake pad to innovation accelerator

Markus Limbach
Partner, Consulting,
Cyber Security & Resilience,
KPMG AG Wirtschaftsprüfungsgesellschaft

In the dynamic world of cloud technologies, security is often perceived as a necessary evil or even a potential brake on innovation. But this perspective is outdated. In view of the increasing complexity of multi-cloud environments and the growing threat landscape, cloud security must be seen as a strategic enabler that creates trust and enables digital transformation.

Shift-Left-Security and DevSecOps as standard practice:
The traditional practice of looking at security at the end of the development cycle is untenable in cloud-native environments. "Shift-left security" means integrating security aspects into the entire software development lifecycle (SDLC) right from the start. DevSecOps as a methodical approach promotes collaboration between development, operations and security teams. This leads to proactive identification and remediation of vulnerabilities before applications go into production and reduces the risk of costly rework and security incidents. It is a fundamental shift towards "security by design".

Zero trust architectures as a principle of cloud security:
The traditional "perimeter security model" - according to which everything within the network is trustworthy - is obsolete in cloud and multi-cloud environments. Zero Trust establishes the principle that no user, device or application is implicitly trustworthy, regardless of its location. Every access attempt is explicitly authenticated, authorized and continuously validated. This is crucial to protect the complex attack surfaces in distributed cloud architectures and minimize the threat from internal and external attackers alike. Identity and access management (IAM) thus becomes the core of the security strategy.

Automation and AI-supported security operations (SecOps):
Given the sheer volume of security events and the speed of cyberattacks, purely manual security monitoring is no longer practicable. The future of cloud security lies in the automation of threat detection, analysis and response. response to threats. AI and machine learning are used to detect anomalies in huge amounts of data, analyze behavioral patterns and take preventive measures. This allows security teams to focus on more complex threats while drastically reducing response times. Automated remediation and self-healing systems are becoming the norm.
the norm.

Cross-connections and implications:
A robust cloud security strategy is the foundation f o r success in all other areas. Without confidence in security, companies cannot fully develop their AI strategies, especially if they process sensitive data. A secure multi-cloud environment requires the consistency and automation e n a b l e d by DevSecOps and Zero Trust. The efficient use of the public cloud also depends to a large extent on an intelligent security architecture that uses and extends the native security functions of the providers. The integration of AI into SecOps is a prime example of how technologies reinforce each other.
In short: security is not a downstream task, but must be considered as an integral part of the overall cloud strategy from the outset and continuously developed further. It is the guarantee that companies can exploit the opportunities of digital transformation securely and confidently.

04

FinOps and cost management

Many companies are turning to the cloud to increase efficiency and reduce costs. In practice, however, the picture is more nuanced: cost savings often fall short of expectations, and early savings effects have already been exhausted in many places. While the cloud was long regarded as a source of rapid cost benefits, it has developed into a strategic discipline that is associated with increased complexity and rising demands on governance, FinOps and transparency. If you want to save money in the future, you need to actively manage cloud costs. A robust, cross-team FinOps framework is crucial here. The sovereign cloud is also gaining financial importance: it is increasingly seen as a necessary added value for which many companies are willing to pay a substantial premium.

4.1 FinOps enables long-term cost savings when using the cloud

- Noticeable IT cost savings through cloud use are reported by 61% of the companies surveyed. In 2024, the figure was 67%.
- Large companies (62%) are more likely to see cost savings in IT than companies with 50 to 249 employees (55 percent).
- A total of 42 percent invest around half of their IT budget in cloud spending and 36 percent around a quarter.

across the board. For example, 61% of the companies surveyed reported noticeable savings in internal IT costs through cloud use. Large companies in particular, which are more strongly represented in this survey than in the market as a whole, report lower costs. While this figure still accounts for a significant proportion, it represents a decrease of six percentage points compared to the previous year. A good one in five companies (21%) see no impact on their IT costs as a result of cloud use. Initial savings effects have often been exhausted. For long-term sustainable cost management, companies must therefore actively manage the cloud and align it economically in order to balance the relationship between costs and benefits.

Cloud usage therefore remains a key tool for cost optimization, but the early benefits are decreasing noticeably. Expectations of immediate cost benefits from cloud use are therefore becoming more relative. As cloud maturity increases, additional cost factors arise, such as for management, monitoring and compliance. Without clear control, these can quickly lead to additional costs. Price increases and additional services offered by providers at extra cost further reduce existing benefits.

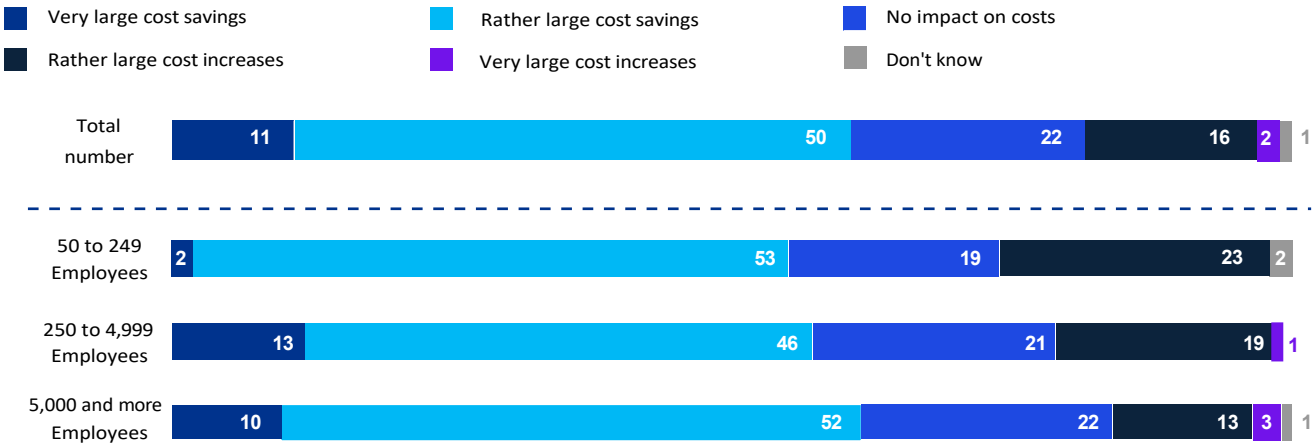
However, there are differences depending on the size of the company. While 62% of large companies (5,000 or more employees) notice significant cost savings, only 55% of companies with 50 to 249 employees do. Larger companies benefit more from scaling effects, volume-based price models and standardized processes.

Cloud expenditure is largely in the middle of the IT budget. For 42% of companies, around half of IT costs are attributable to cloud expenditure and for 36% around a quarter. The cloud is therefore an integral part of financial planning for 78% of companies, but does not dominate the budget. Strict planning is still required to ensure that these proportions do not increase.

FinOps is the key to sustainable cost management. Transparency about consumption, binding budgets and company-wide cost discipline make the difference between cloud as an efficiency driver and cloud as a cost driver. Cost-efficient cloud usage requires interdisciplinary, specialized personnel with cloud expertise and FinOps knowledge. If companies want sustainable cost benefits, they therefore need FinOps discipline, governance and a clear roadmap in which costs are systematically planned from the outset.

How has cloud use affected IT costs in your company?

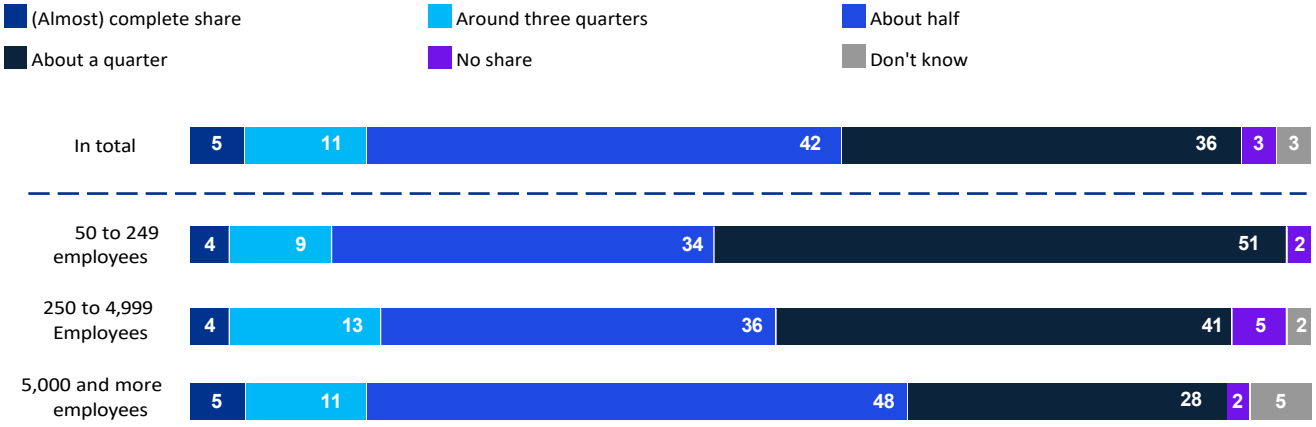
Figure 13:
Impact of cloud use on IT costs by company size



Percentage of companies that use cloud services, n = 509, by company size n = 47/216/246 | Totals deviating from 100 percent are due to rounding differences.
Source: KPMG in Germany, 2025

What proportion of your company's total IT expenditure is spent on cloud IaaS, SaaS and PaaS?

Figure 14:
Share of cloud costs in the IT budget by company size



Percentage of companies using cloud services, n = 509, by company size n = 47/216/246 | Totals deviating from 100 percent are due to rounding differences.
Source: KPMG in Germany, 2025

4.2 The sovereign cloud is gaining in importance. Companies are willing to pay a premium for it

- The vast majority of companies (98%) signal their willingness to pay a premium for a sovereign cloud.
- A total of 44% of the companies surveyed would pay a surcharge of up to 20% for a sovereign cloud. One in ten companies would even pay a surcharge of more than 30 percent.
- A slightly lower surcharge (up to ten percent) would be paid by 22 percent of the companies surveyed.

The sovereign cloud is becoming a key strategic technology, especially for industries in which sensitive data, intellectual property or critical supply chains need to be protected. For many companies, sovereignty 2025 is a decisive added value for which they are also considering investing additional budget: 22 percent of companies would pay up to ten percent more and 44 percent would consider an additional charge of up to 20 percent into consideration.

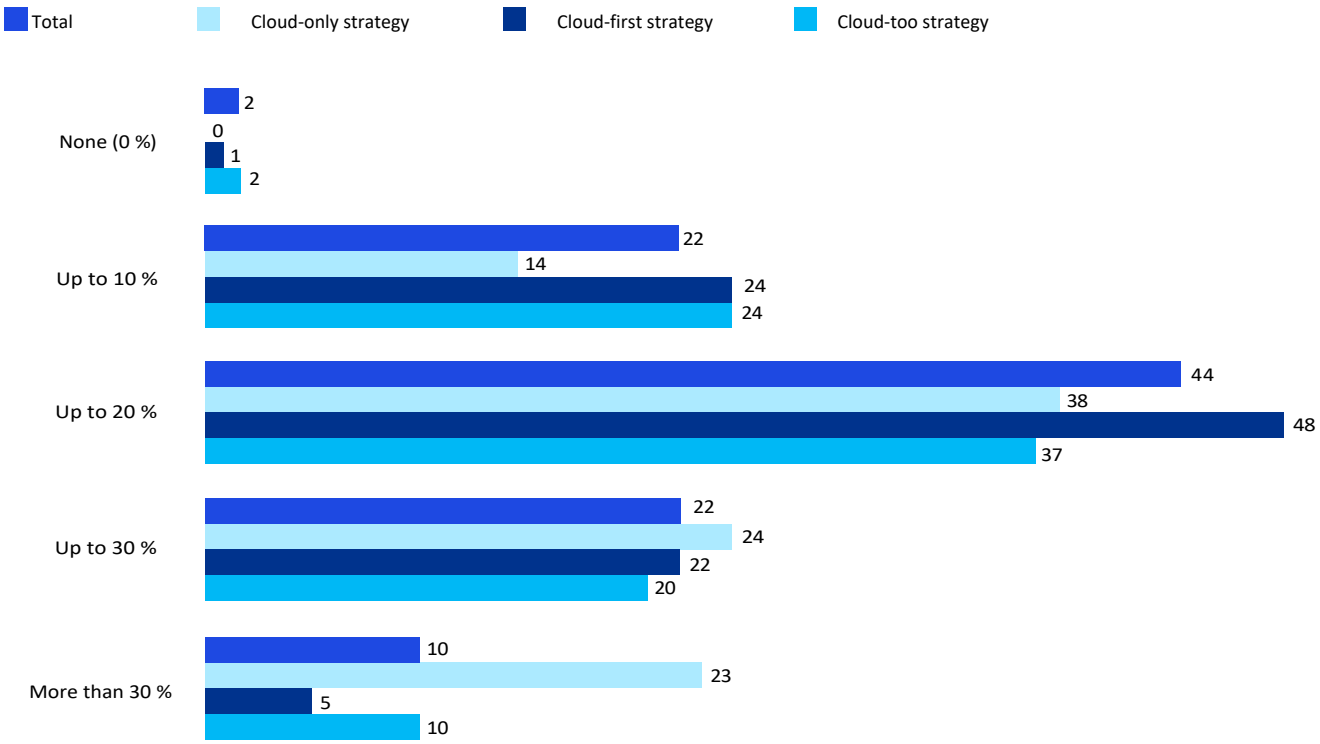
Sovereignty is thus developing from an additional option to a strategic must. One in ten companies is even considering a surcharge of over 30 percent. For companies with cloud-first strategies, however, at five percent this willingness is significantly lower than the average across all cloud strategies. This shows: The perceived added value depends heavily on the use case and industry-specific requirements. Sovereign clouds can be more popular in highly regulated industries or at companies with a lot of sensitive data, as they support improved control over data sovereignty and access rights.

European challengers and US hyperscalers are competing US hyperscalers are competing with different concepts. European providers are convincing due to their greater legal autonomy and reduced third-country risk. However, hyperscalers often offer more comprehensive services and can score points with their innovative strength thanks to modern technology platforms.

A practicable approach combines data protection with economic viability. Providers must translate the added value of regulatory compliance into feasible and scalable pricing models so that costs do not become an obstacle to implementation. On the corporate side, the use of the cloud requires a well thought-out operating model. This allows companies to carefully examine the extent to which their industry or specific use cases are suitable for operation in the sovereign cloud with European providers, or whether they want to take advantage of the scalability of hyperscalers. Those who master this balance will remain competitive in the long term while maintaining a high level of data protection.

What surcharge do you consider appropriate for a sovereign cloud?

Figure 15:
Willingness to pay a premium for a sovereign cloud according to cloud strategy



Percentage of companies that use cloud services by cloud strategy n = 78/318/95/ | Missing at 100 percent = "I don't know."
Source: KPMG in Germany, 2025

4.3 Cloud spending is forcing companies to rethink cost management

- The biggest challenge in cloud cost management in 2025 is the reduction of waste (31%) (2024: 26%).
- In each case, 24% struggle with accurate spend forecasting, spend allocation and automation.
- The challenge of winning over developers and (DevOps) engineers for cost optimization has decreased significantly: From 28 percent in the previous year to 22 percent this year.

Cloud cost management has matured into a strategic discipline that makes the difference between efficiency gains and rising expenditure through transparency, governance and automated control. However, companies are facing structural challenges, particularly in terms of processes and coordination. At the same time, a cultural change in companies is giving rise to confidence: specialist departments are increasingly taking on financial responsibility.

Companies are struggling to keep an eye on unused resources and actively manage their expenditure. Wasting resources is therefore at the top of the list of challenges to be mastered at 31 percent. Companies see the greatest leverage in unused or incorrectly dimensioned instances. Cost risks arise from variable billing models, dynamic scaling and complex multi-cloud setups, as these can result in excessive resource provisioning, idle times or a lack of transparency. The waste of resources thus becomes a structural problem.

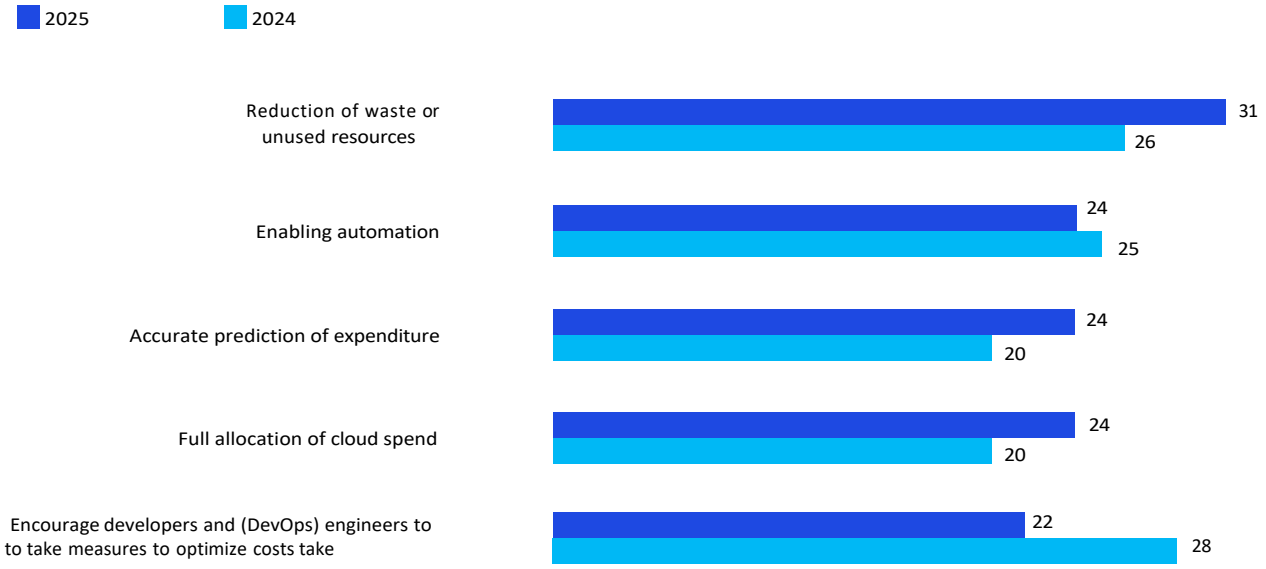
Optimization potential in cloud cost management is also evident in company-wide coordination. In each case, 24% of all companies surveyed have difficulties with accurate expense forecasting, expense allocation and automation. Cloud cost management and FinOps remain particularly challenging in terms of transparency and forecasting capability. These structural, organizational bottlenecks also affect other areas of cloud usage. It was already clear from the hurdles of public cloud use, such as process and system adjustments (see section 2.2), that companies struggle most with adapting their structures. This trend is now continuing with FinOps challenges. Companies must therefore act across departments in order to overcome complex cloud obstacles.

At the same time, a change in corporate culture is emerging. Developer and DevOps teams are increasingly taking active responsibility for costs, so that optimization begins in the development process and FinOps is understood across the board. Only 22 percent still find it challenging to convince developers and engineers to optimize costs - a decrease of six percentage points compared to the previous year. Awareness of cost efficiency is therefore also increasing among dev teams and FinOps principles are beginning to establish themselves across teams.

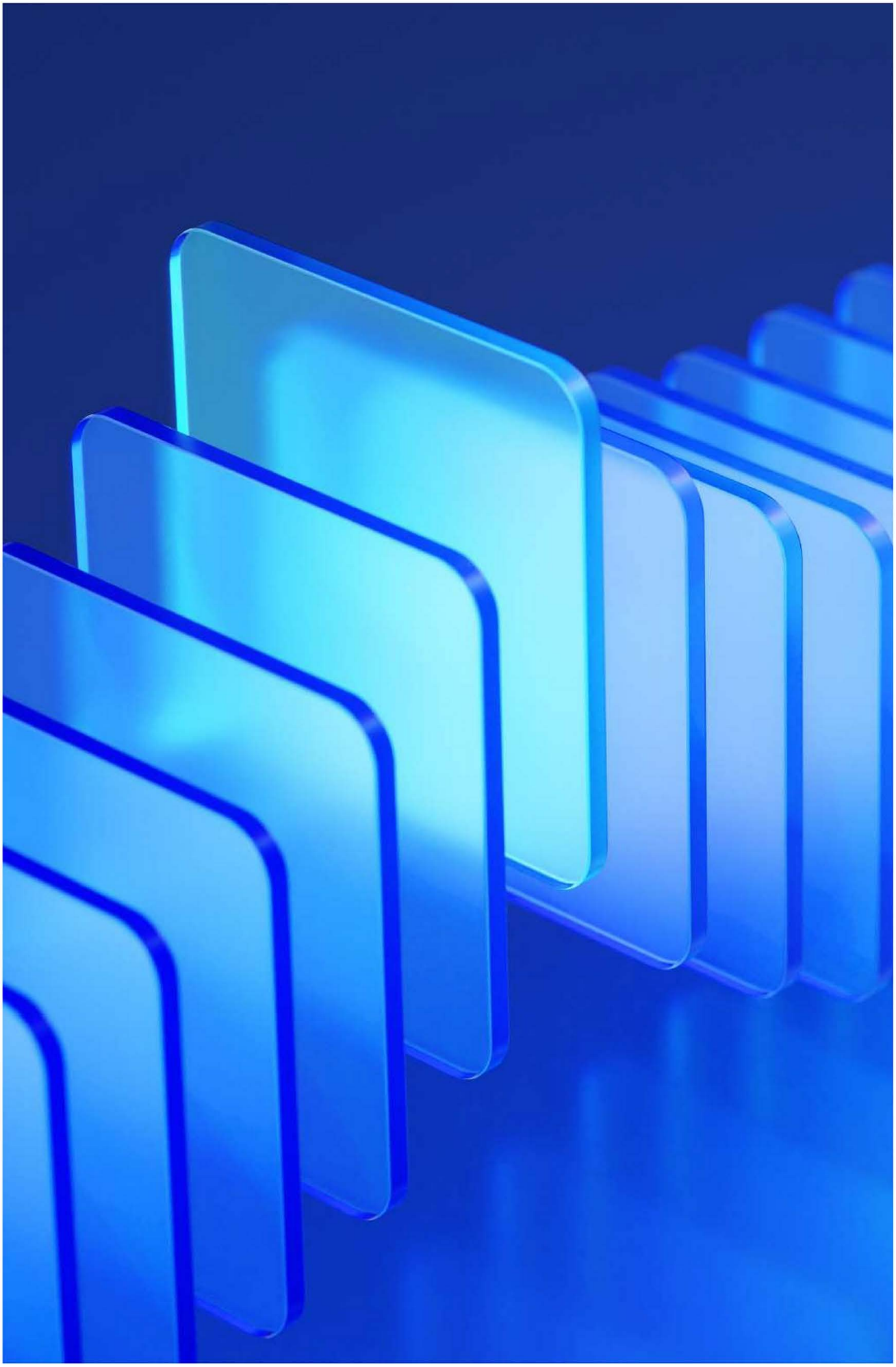
A consistent FinOps governance framework that dovetails technical measures with financial and compliance processes creates a resilient foundation for further cloud growth at sustainable costs.
A framework of this kind unfolds its full benefits when responsibilities, key figures and training are established throughout the organization.

What are the three biggest challenges in cloud cost management for your company?

Figure 16:
Top 5 challenges in cloud cost management in a year-on-year comparison



Percentage of companies that use cloud services, by survey year (2024/2025) n = 503/509 | Multiple answers possible (maximum 3 answers).
Source: KPMG in Germany, 2025



FinOps and cost management: making intelligent use of cloud potential

Martin Wißkirchen
Partner, Consulting,
Technology Strategy & Operations
KPMG AG Auditing Company

Migration to the cloud promises cost savings and efficiency gains. However, the reality often shows that cloud costs can escalate quickly without proactive management. This is where FinOps comes in: It's not just a set of tools or processes, but a culture that combines financial responsibility with technical agility to extract maximum business value from cloud investments.

Three key trends are shaping this field:

FinOps as a collaborative corporate culture: the shift from purely technical cost management to a collaborative culture is crucial. FinOps promotes collaboration between finance, IT and development teams to define common goals and optimize cloud usage in a data-driven way. It's about creating transparency around costs and giving each team the tools and responsibility to understand the financial impact of their decisions. of their decisions. Only when developers who provision resources also know the costs can sustainable optimizations be achieved.

Automated cost optimization and governance:
Given the dynamics and complexity of cloud environments, manual cost management is inefficient. The trend is towards automated solutions that analyse cost patterns, identify waste (e.g. unused instances, overdimensioned resources) and make suggestions for optimization or even implement them automatically. This also includes the automated enforcement of governance rules, such as the automatic scaling down of unused environments or the use of reserved instances/savings plans. Machine learning is playing an increasingly important role here in order to identify anomalies and optimization potential.

Value-oriented cloud management beyond pure cost reduction:
FinOps overcomes the pure focus on cost reduction and puts business value at the center. The aim is to maximize the return on investment (ROI) of cloud expenditure by putting costs in relation to the value generated. Decisions are not only made based on the lowest price, but on the best price-performance ratio for the business requirements. This requires metrics that reflect both technical performance and business value, and a continuous assessment of how cloud resources can most effectively contribute to strategic goals.

Interconnections and implications:
An effective FinOps strategy is closely linked to the strategic use of the public cloud and the mastery of multi-cloud strategies. Without clear visibility and control over spend, t h e benefits of cloud scalability and flexibility can quickly be eaten up by uncontrolled costs. The findings from FinOps can also influence cloud strategies by showing which workloads can be operated most cost-effectively in which cloud environment (e.g. multi-cloud approaches). In addition, FinOps creates the financial basis for investments in new technologies such as AI initiatives by ensuring that the cloud infrastructure is operated efficiently and in a value-oriented manner. It is a continuous process of optimization and learning that plays a crucial role in the long-term success and sustainability of cloud investments. Companies that do not establish FinOps as the core of their cloud governance risk not only unnecessary expenditure, but also the ability to exploit the full innovation potential of the cloud.

05

Data and AI

In addition to analytics solutions, companies are increasingly using AI-supported language models for data-driven business and decision-making processes. AI opens up new possibilities in data processing by also being able to analyze and condense unstructured data, making it easier to derive actionable insights. The majority of companies rely on large language models (LLMs) to quickly analyze large amounts of data and automate routine tasks. The survey shows: Respondents often pursue a multi-LLM approach. When using generative AI, the first companies are already using AI-based compliance and performance monitoring.

Hosting - of both analytics applications and AI - is primarily carried out by large providers who develop their own language models themselves or have them developed by partners.

This has an impact on the hosting landscape and reinforces the shift from traditional data centers to large hyperscalers, where data, computing power and services are centrally available. Traditional data centers are becoming less important for the majority of companies.

5.1 Hyperscalers benefit from data analytics solutions

- The most frequently used analytics solutions are hosted in hyperscaler clouds (Microsoft: 54 percent, Amazon Web Services (AWS): 50 percent, Google Cloud Platform (GCP): 44 percent).
- SAP Analytics Cloud is the only specialized provider among the five largest platforms for analytics applications (44%).
- Only seven percent of companies still use on-premise environments for analytics solutions - a sharp decline compared to 2024 (16 percentage points).

Companies primarily host their analytics solutions in the cloud and are increasingly moving away from their on-premise environments: Only seven percent of companies will still use the traditional data center for hosting in 2025, a decrease of 16 percentage points compared to 2024 (23 percent).

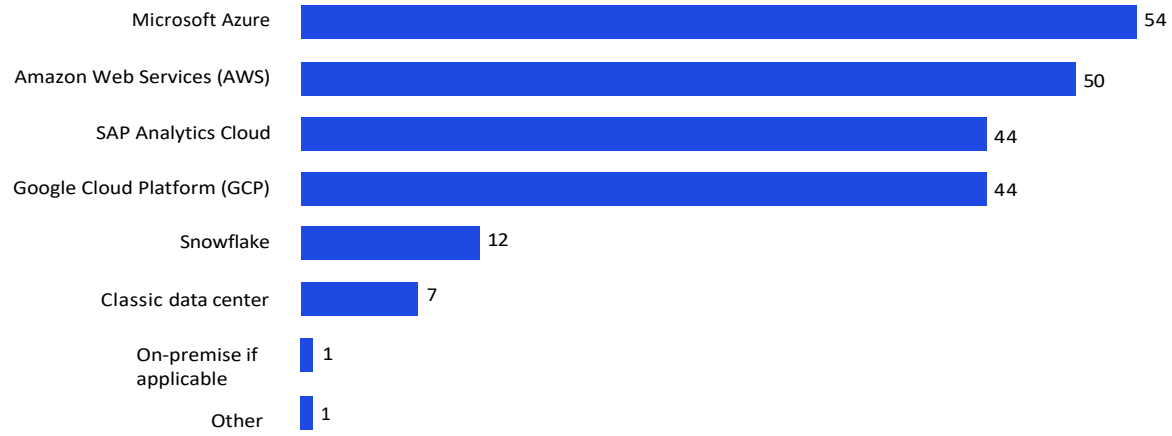
Analytics solutions are most frequently hosted by the hyperscalers Microsoft Azure (54%) and AWS (50%). This comparably high usage suggests that companies prefer to operate their analytics stacks with providers that already host their data and operate workloads. In addition, the performance of the stacks and the prices also play a significant role with AWS, for example. The existing infrastructure has a decisive influence on the choice of analytics solutions in companies, which means that the dominant hyperscalers in particular can continue to assert themselves.

GCP, where 44% of companies have their analytics solutions hosted, is also benefiting from this trend. Google's success in this area, but also the strong position of other hyperscalers, is likely to be closely linked to the growing spread of cloud-first strategies: many companies that already rely on cloud infrastructures initially established Google for cloud operations and later added analytics and other functions.

SAP Analytics Cloud is the only specialized platform to make it into the top five providers with 44%. In Germany, business analytics is traditionally regarded as an SAP domain, but SAP was comparatively late to enter the market with its cloud solution only entered the market comparatively late and therefore lost important usage shares to the American hyperscalers. Despite the late entry, SAP has been relatively successful with its analytics solution, as the Walldorf-based company can score points with its seamless integration into the widely used SAP systems. In particular, companies that do not yet have an established cloud structure often choose SAP as a complete solution that closely integrates analytics and ERP functions. The comparatively strong spread of SAP Analytics in the cloud is therefore also likely to stem from the pattern described above: Companies prefer data analysis tools in a familiar environment.

Where does your company source modern analytics solutions from?

Figure 17:
Source of analytics solutions



We do not use analytics solutions[1]

Percentage of companies that use cloud services, n = 509 | Multiple answers possible.

[1]*Exclusive response.*

Source: KPMG in Germany, 2025

5.2 LLMs are an integral part of company-wide processes

- Large Language Models (LLMs) are used by 92% of the companies surveyed.
- OpenAI's GPT remains the clear leader among LLMs, with 61% of companies using the system.
- In second place is Google's LLM-based application Gemini with 40 percent usage.

In addition to the use of analytics solutions, companies are increasingly using AI to analyze huge amounts of unstructured data or to derive relevant insights with concise summaries. LLMs play a key role in this: already 92 percent of respondents use LLMs in their daily work or have implemented initial integrations of LLMs into their business processes. This can refer to the use of LLMs by individual employees as well as their strategic use in companies. The great popularity of LLMs can be explained by their wide range of possible applications, such as the translation of huge amounts of data into usable knowledge or the automation of routine tasks, research or text creation.

Many companies rely on the broad use of LLMs - often even on several models in parallel in order to make optimum use of the strengths of different systems. A total of 69 percent of LLM users pursue a multi-LLM approach instead of committing to a single provider. It makes sense to make a selection b a s e d not only on technical criteria, but also on the specific requirements of the respective use cases.

Among the LLMs used, GPT is the clear leader with a usage rate of 61 percent. GPT is also integrated in Copilot and is used by companies primarily to support research and writing tasks. Gemini follows in second place with a gap of more than 20 percentage points. The Google-based solution is used by 40 percent of the companies surveyed and is characterized by its flexibility across different platforms. The use of these two LLMs varies significantly depending on the size of the company. For example, 71 percent of companies with 5,000 to 9,999 employees use GPT. Companies with 50 to 249 employees, on the other hand, are above the average for Gemini (47%).

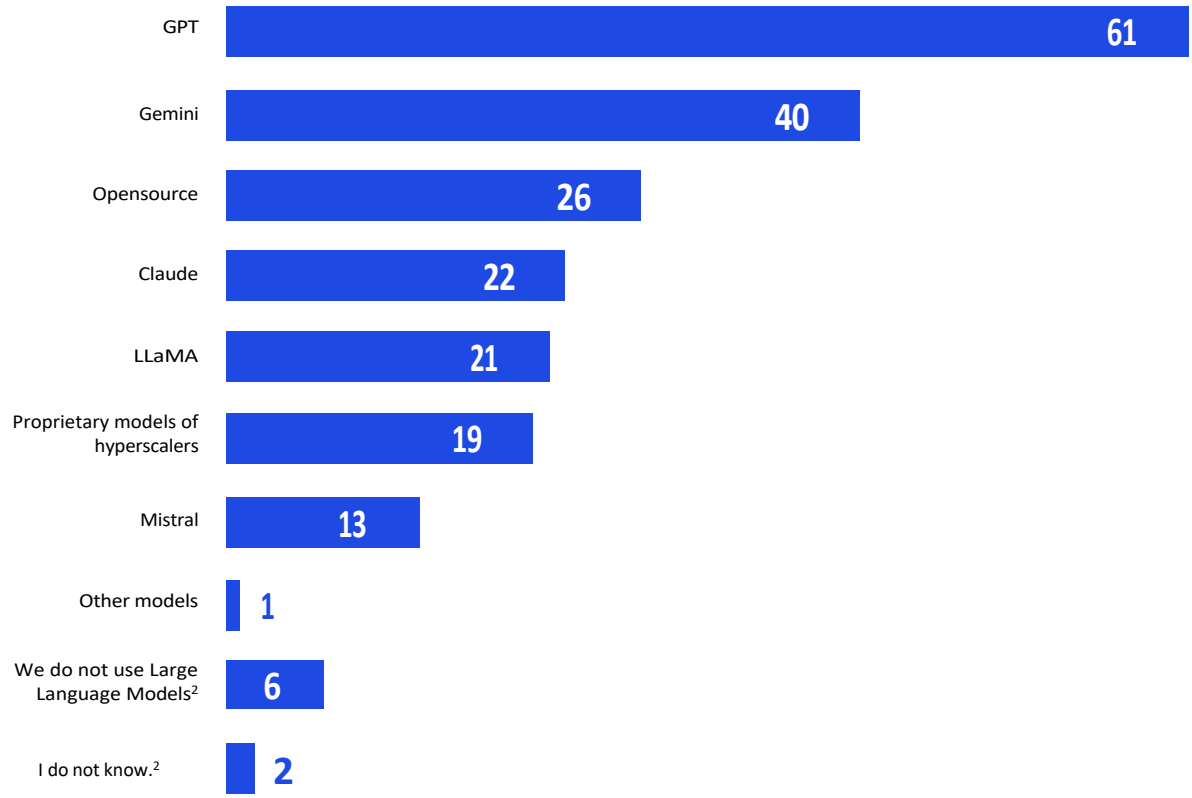
Over a quarter (26%) also use open-source solutions, primarily for reasons of digital sovereignty and to avoid vendor lock-ins. However, investment costs in hardware must be borne by companies in advance. It is important to realistically calculate the actual costs for a potentially more complex in-house operation.

The adoption rate and usage intensity of LLMs will continue to rise in 2025, albeit only in small steps. Compared to the previous year, the proportion of companies not using LLMs fell by four percentage points, while the usage rates of ChatGPT, Gemini, Claude and LLaMA each increased by two to four percentage points. This shows that even latecomers are now actively taking up the topic and existing users are increasingly o p t i n g for a multi-LLM approach.

In view of this high technological penetration, LLMs are increasingly becoming a hygiene factor. The focus is increasingly shifting from technological aspects to the human factor: employees must be qualified and continuously trained in the competent use of LLMs. It is also advisable to regularly evaluate the intensity of use and potential of LLMs in your own company and, if necessary, initiate measures to promote them in order to secure your own competitiveness in the long term.

Where does your company source large language models from?

Figure 18:
Source of large language models



Percentage of companies that use cloud services, n = 509 | Multiple answers possible.
[2]Exclusive response
Source: KPMG in Germany, 2025

5.3 Generative AI is being tested in practice:The first companies are already testing complex fields of application for generative AI

- Copilot (38%) and generative AI chatbots (35%) are the most frequently used methods and techniques in the field of generative AI.
- 29 percent of the companies surveyed use AI-based performance monitoring to monitor the use of AI solutions. AI-based compliance monitoring to meet the compliance requirements of AI chatbots is used by 26 percent.
- 96% of cloud-using companies obtain modern AI solutions from cloud providers. Only 13% still use on-premise solutions - 13 percentage points less than in the previous year.

Generative AI is currently being used in many companies primarily for end-user tools that increase personal productivity: 38% use Copilot and 35% use generative AI chatbots. Many companies are also developing their own AI chatbots based on GPT, which are cheaper to use than Copilot. Both copilots and AI chatbots are easy to use, deliver rapid efficiency gains and often serve as a starting point f o r gaining experience for later automation and more complex use cases.

Another important field of application is performance and compliance monitoring, which is currently used primarily in conjunction with AI tools to increase personal productivity and at the same time to ensure compliance with legal and ethical requirements.

is a lever for greater business performance. Performance monitoring checks the performance of AI applications and also evaluates whether the expected efficiency gains are actually being achieved. Twenty-nine percent of the companies surveyed already rely on AI-based performance monitoring, and this figure rises to 35 percent for companies with cloud-first strategies (cloud-only: 19 percent, cloud-too: 18 percent). Particularly in hybrid architectures with cloud and on-premise components
AI-based monitoring is in demand, as the complexity of the systems is higher here and transparency regarding utilization and availability is difficult to guarantee manually.

To ensure compliance with legal and ethical requirements, 26% of respondents use AI-supported compliance monitoring. In contrast to traditional approaches, checks are continuous, automated and significantly less prone to errors. Especially where people interact directly or indirectly with AI, risks can be identified at an early stage and regulatory requirements can be monitored efficiently. In the long term, however, the mechanisms used today are also likely to become standard for process AI, automation and multi-agent systems.

The combination of AI, low-code, SaaS and RPA, which 25% of companies are already using, represents a further step towards business productivity. It accelerates the automation of routine tasks such as data entry, approvals or reporting and enables specialist departments to adapt workflows without in-depth IT expertise. This makes processes more flexible and innovations can be transferred to everyday operations more quickly.

The use of agentic AI is still in its infancy. For example, 17% of companies state that they use such systems, while 22% are experimenting with multi-agent systems. These are often

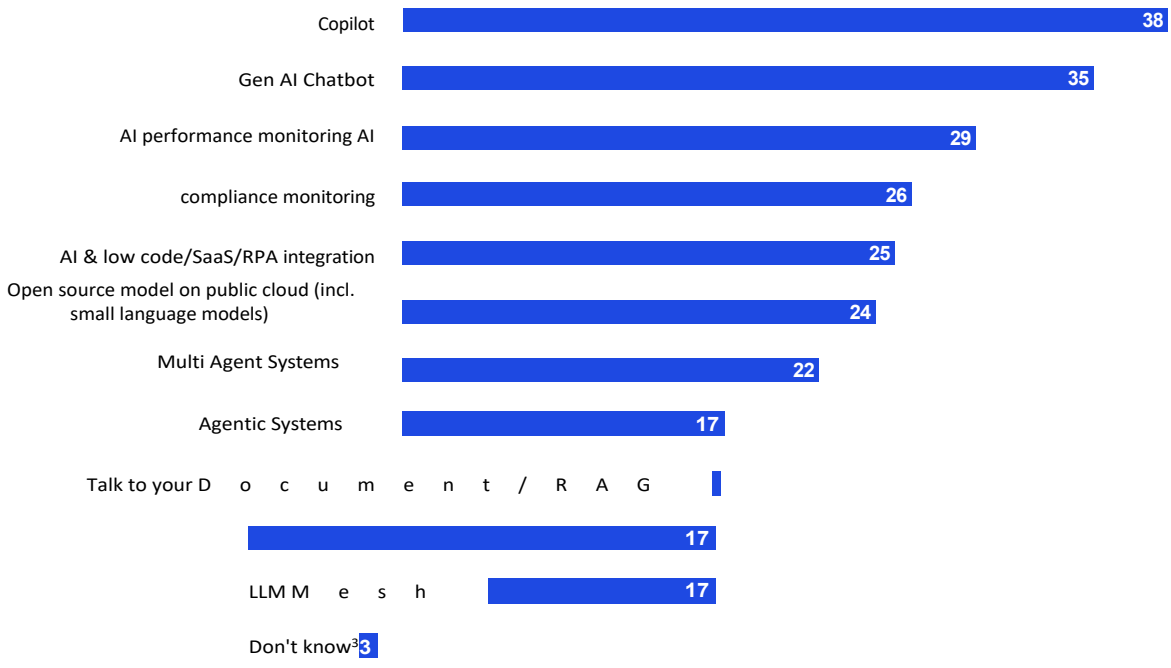
hybrid approaches that combine classic automation with generative AI - without producing an AI with genuine autonomous decision-making or action capability. However, some solutions are often incorrectly referred to as agentic AI, although the orchestration of processes is still implemented in the traditional way. The full performance promise of this technology has not yet been fully exploited, especially at present due to the lack of interfaces. Nevertheless, the growing interest shows that companies are already laying the foundations to benefit from Agentic AI in the future - for example, through autonomously acting systems that not only perform complex tasks, but can also strategically plan and optimize them.

Companies primarily host their AI solutions with large hyperscalers - regardless of whether these are solutions from the hyperscalers themselves or from other providers. Microsoft Azure is in the lead with 57%, followed closely by GCP and AWS with 52% each. All three providers show slight growth of two to four percentage points. The number of companies using each platform was recorded and not the proportion of companies using it, meaning that the level of expenditure cannot be derived from this. It is also a survey of general usage and not the primary platform used. The increasing prevalence of large providers can be explained by the fact that companies rely on established partnerships for AI hosting: They often use existing infrastructures and build their
AI stacks where data and workloads are already located.

While hyperscalers are benefiting from this dynamic, the traditional data center is becoming less important - only 13% of companies are still using their own infrastructures, half as many as in the previous year. In addition to more mature technologies, the reasons for this include an increased level of maturity among companies and a growing demand for AI in specialist areas.
for AI in the specialist areas.

Which methods and technologies in the field of GenAI are u s e d in your company?

Figure 19:
Top 10 methods and techniques in the field of GenAI

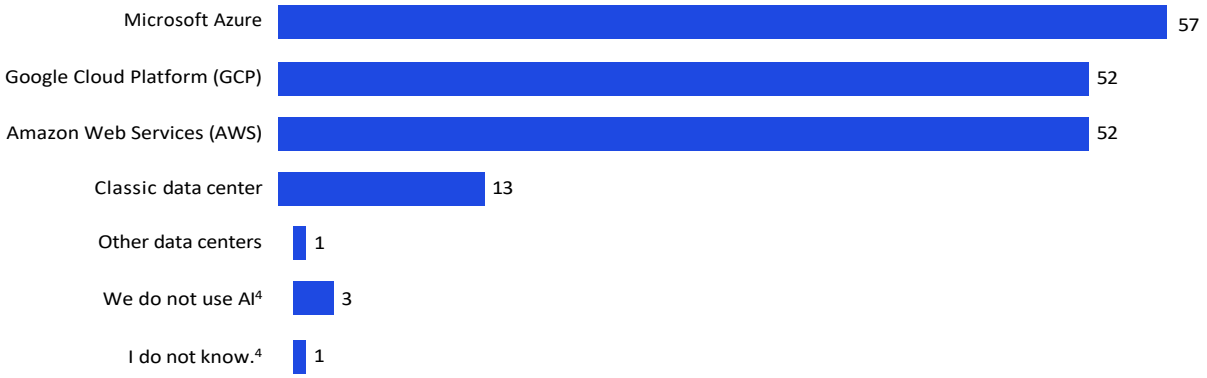


Percentage of companies that use cloud services, n = 509 | Multiple answers possible.

[3]*Exclusive response.*
Source: KPMG in Germany, 2025

Where does your company source modern AI solutions from?

Figure 20:
Source of AI solutions



Percentage of companies that use cloud services, n = 509 | Multiple answers possible.

[4]*Exclusive response*

Source: KPMG in Germany, 2025

Data and AI: the symbiosis of digital value creation

Michael Niederée
Partner, Consulting,
Technology Transformation,
KPMG AG Wirtschaftsprüfungsgesellschaft

The inextricable link between data and artificial intelligence (AI) is at the epicenter of digital transformation. While data serves as the raw material, AI is the engine that converts this raw material into intelligence and ultimately into business value. Companies that master this symbiosis are able to revolutionize decision-making, optimize processes and create entirely new products and services.

Data Fabric and Data Mesh as architectures for data accessibility and governance: Traditional, monolithic data architectures are often too rigid to meet the requirements of agile AI projects. The trend is moving towards more flexible approaches such as data fabric and data mesh. A data fabric creates an integrated data layer across different data silos to simplify data access and integration. A data mesh decentralizes data ownership and promotes data product-centric thinking, where data-owning teams are responsible for delivering high-quality, easily consumable data products. Both approaches aim to improve data accessibility and create a solid data foundation for AI applications while ensuring governance and quality.

The rise of generative AI and the scaling of enterprise AI:
Beyond traditional machine learning (ML) applications, generative AI is rapidly gaining in importance. From automated content creation and software development to the personalization of customer experiences, generative AI is opening up completely new fields of application. At the same time, the focus is increasingly on scaling AI initiatives across the entire company ("enterprise AI") in order to overcome isolated pilot projects and integrate AI into core processes. This requires not only advanced models, but also robust machine learning operations (MLOps) practices to effectively manage the lifecycle of AI models.

Responsible AI and AI governance as the cornerstone of trust:
As the performance of AI systems increases, so do the ethical and social issues. The trend is towards the establishment of
"Responsible AI" and comprehensive AI governance frameworks. This includes ensuring fairness, transparency, explainability and accountability of AI models. Companies are required to develop guidelines for the ethical use of AI, identify and mitigate bias in data and algorithms and ensure compliance with relevant regulations. This is the only way to build trust in AI systems and promote their acceptance.

Cross-connections and implications:
The effectiveness of AI strategies depends directly on the quality and accessibility of the data, which is improved by Data Fabric and Data Mesh. The computing power and scalability required for the training and operation of generative AI is largely provided by public cloud computing and an intelligent multi-cloud strategy. The edge cloud (Op-Ed 2) also plays a role in the collection and pre-processing of data for
AI applications, particularly in the IoT area. Robust cloud security measures are essential in order to operate these complex AI and data landscapes securely. Investments in data and AI infrastructure must be accompanied by efficient FinOps practices to extract maximum value from these strategic assets. Successfully integrating these areas is critical to fully harnessing the transformative power of data and AI and enabling organizations to thrive in a data-driven world. It is about developing a coherent strategy that encompasses technology, processes, governance and ethics to realize the full potential of these key technologies.

Conclusion and recommendations

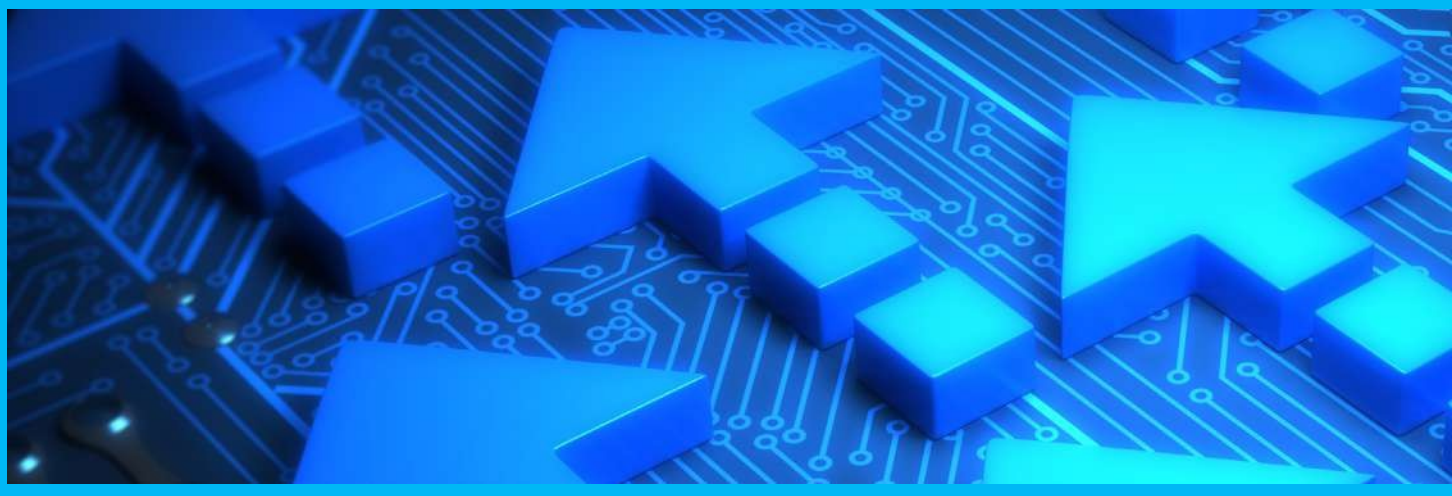
The increasing share of public cloud usage reflects the growing digital maturity of companies. At the same time, many companies will face a volatile situation in 2025. Technological diversity meets cost pressure, regulation and a shortage of skilled workers. Companies must strategically align their cloud architecture, FinOps, security and AI integration for flexibility and value creation. Companies can achieve sustainable, economically viable cloud migration through holistic governance.

Sharpening public cloud roadmaps for agility

Cloud usage is evolving from an infrastructure option to a strategic driver for agility. Hybrid operating models with a clear tendency towards the public cloud predominate, with companies consciously orchestrating multiple providers in order to balance innovative strength, cost efficiency and sovereignty. However, public cloud usage is not growing to the extent that it could.
Companies should therefore define their cloud roadmap with clear migration strategies today. At the same time, they need to strategically design their provider partnerships and check their performance and security. This will turn the cloud into a robust platform for sustainable growth and digital transformation.

Holistic implementation of cloud security with Zero-Trust

Regulatory pressure, threats and heterogeneous IT landscapes will make cloud security an ongoing strategic task in 2025. NIS2, the EU AI Act and industry-specific requirements are forcing integrated governance structures that address data protection and compliance as well as operational resilience. Companies are responding to these developments with proactive security concepts and the expansion of zero-trust services. It is advisable to integrate compliance at an early stage and modernize infrastructures step by step at the same time. The combination of modern methods and simultaneous legacy compatibility ensures digital resilience and creates robust security architectures.



FinOps anchoring and strategic use of the Sovereign Cloud

Increasing complexity and decreasing short-term effects make cloud costs a central management task. A resilient FinOps framework is needed for the cloud as an efficiency driver rather than a cost driver. At the same time, the importance of sovereign cloud offerings as a targeted response to compliance and data protection requirements is growing. Companies are signaling their willingness to accept moderate surcharges for this, but expect measurable added value through regulatory security and value-adding services.

A dual approach is expedient here. Companies should establish FinOps as a company-wide discipline with clear responsibilities. At the same time, they can segment their productive applications systematically. Business-critical or highly sensitive data is then stored in the sovereign cloud, while scalable standard loads remain with the hyperscalers. Companies secure their financial and technological room for maneuver by using three levers: They firmly anchor FinOps in their processes, qualify their teams and drive a differentiated multi-cloud strategy.

Strategic orientation for the future of AI

The German corporate landscape is seeing an increasing adoption rate of AI use, which is likely to come to a head in the coming years.
Multi-cloud architectures and a portfolio of different LLMs will become the de facto standard. At the same time, there is a trend towards cloud-native analytics and AI services being preferably hosted on hyperscaler clouds and on-premise environments being scaled back further.

Generative AI is currently used primarily via easily integrated end user tools and is supplemented by AI-based performance and compliance monitoring.
Although Agentic AI is still at an early stage, companies are showing interest. Those who prepare the architecture, interfaces and orchestration today can accelerate future production scenarios.

Digital future potential

Companies are implementing their increasing level of digital maturity: The majority of companies plan to run their productive workloads primarily in the public cloud by 2028. At the same time, generative AI is used in a variety of ways and is primarily cloud-based. The move towards the public cloud requires a holistic transformation of skills, culture and processes. If companies understand governance, FinOps, security and AI strategy as an integrated system, they will lay the foundations for a resilient, innovative and sustainably affordable IT landscape and secure a future-proof market position.

Contact KPMG

KPMG AG
Accounting firm

Gernot Gutjahr
Partner, Consulting
Head of Technology Strategy & Operations,
Head of Managed Services T
+49 30 2068-4495
ggutjahr@kpmg.com

Gerrit Bojen
Partner, Financial Services Head of Technology & Finance Consulting
T +49 89 9282-1076
gbojen@kpmg.com

Wilhelm Dolle
Partner, Consulting, Head of Cyber Security & Resilience
T +49 30 2068-2323
wdolle@kpmg.com

Markus Limbach
Partner, Consulting,
Cyber Security & Resilience T
+221 2073-5833
mlimbach@kpmg.com

Michael Niederée Partner, Consulting, Technology Transformation T +89 9282-4906
mniederee@kpmg.com

Daniel Wagenknecht
Partner, Financial Services T
+49 69 9587-1295
dwagenknecht@kpmg.com

www.kpmg.de

www.kpmg.de/socialmedia