



PwC Cloud Business Survey 2025 Swiss Findings

The new age of cloud:
responding to a shifting paradigm



Content

Key statements	3
About the survey	4
1 Introduction: cloud at a crossroads	5
2 Cloud maturity: from adoption to optimisation	7
3 Geopolitics and regulation: the new cloud borders	17
4 Sovereignty and trust: building resilient cloud strategies	23
5 Agentic AI: the next frontier of cloud intelligence	32
6 Cloud economics: managing the cost of innovation	36
7 Conclusion: embracing the new age of cloud	41
Contacts	43



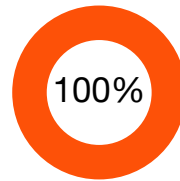


Two years ago, the focus was on moving to the cloud – today, it’s about optimising and adapting cloud capabilities in a sustainable and cloud-native way.

Claudius Meyer

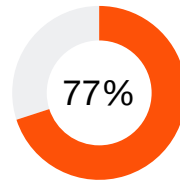
Partner, Cloud, Data and AI, PwC Switzerland

Key statements



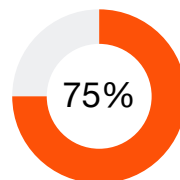
Cloud maturity has advanced rapidly

100% of surveyed Swiss organisations use cloud, up from 77% in 2023 – marking a complete shift to cloud-based operating models and reflecting a clear rise in cloud maturity.



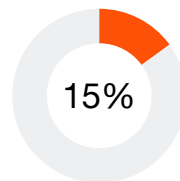
Cloud investments continue to accelerate

77% of Swiss organisations plan to increase their cloud budgets in the next 12 months, up from 60% in 2023 – reflecting sustained digitalisation momentum and ongoing market disruption.



Multi-cloud leads modern cloud strategies

75% of Swiss organisations operate multi-cloud environments to strengthen control, resilience, and regulatory trust while leveraging the best capabilities of each provider.



Agentic AI adoption is still at an early stage

Only 15% of Swiss organisations are implementing or scaling agentic AI – indicating that the next phase of AI-driven cloud maturity is only beginning.



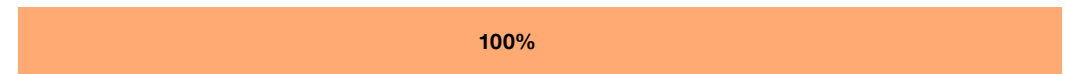
Internal barriers remain significant

Budget constraints, skills shortages, and growing data security and compliance demands are the top obstacles preventing organisations from realising the full value of cloud.

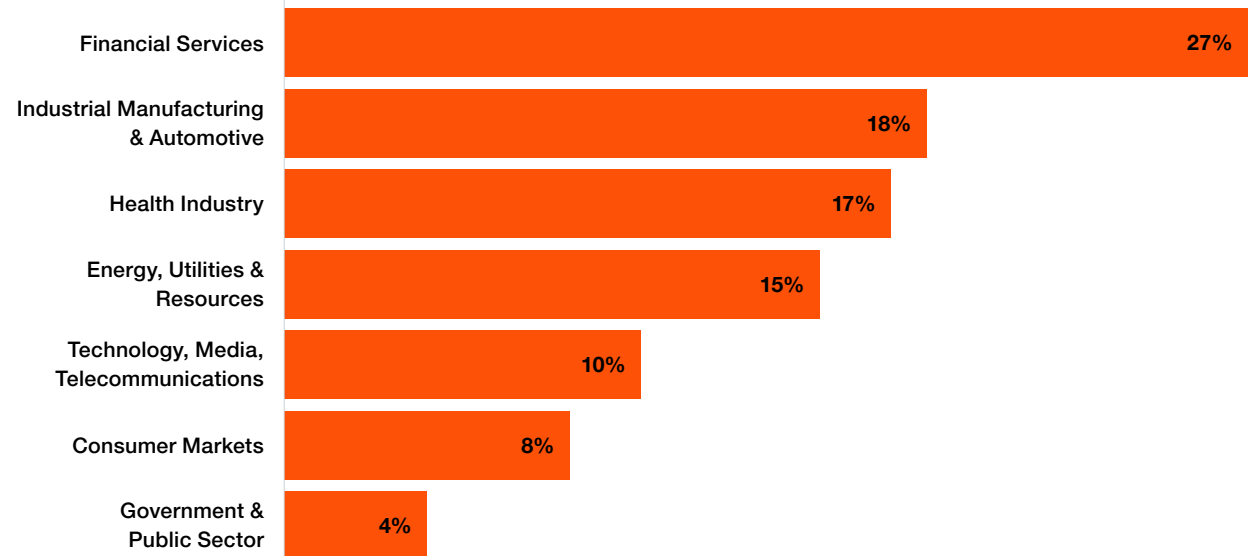
About the survey

Between July and September 2025, PwC surveyed 1,415 business and technology leaders across 26 EMEA territories. Almost half of respondents (44%) come from organisations with annual revenue of USD 1 billion or more. For Switzerland, the dataset includes responses from 71 executives, with an even higher share of large companies: 60% report revenue of USD 1 billion or more. The Swiss sample also spans a broad cross-section of the economy, from financial services and industrial manufacturing to healthcare, energy, technology, consumer markets, and the public sector.

Switzerland: all respondents (71)



Sector: all respondents (71)





Introduction: cloud at a crossroads

Over the past ten years, cloud has shifted from being a scalable infrastructure layer to becoming a core enabler of business transformation. What once served mainly to drive efficiency now underpins innovation, AI adoption and organisational resilience.

At the same time, the context around cloud is changing. Heightened geopolitical tensions, evolving regulation, and rising cost pressures are influencing how organisations plan, build, and govern their cloud architectures. Leaders must navigate the tension between innovation and complexity, ensuring they seize new opportunities while managing risks and meeting sovereignty requirements.



Our survey examines how organisations are adjusting to these new conditions. It highlights five forces shaping the next stage of cloud: the move from broad adoption to optimisation; the impact of geopolitical and regulatory realignment; the growing importance of sovereignty and trust; the emergence of agentic AI; and the rising need to control the cost of innovation through cloud economics. Sovereignty itself spans three dimensions – data, operational, and technology – each essential to ensuring control, compliance, and trust within interconnected ecosystems.

Companies are entering a decisive phase for their long-term strategy. Success will require clear decisions and the ability to leverage AI effectively.



Cloud maturity: from adoption to optimisation

100% of Swiss companies are using cloud, up from **77%** in 2023.

Cloud maturity has risen markedly, with most Swiss organisations now operating at medium or high maturity.

The **top 3** internal barriers to realising cloud value are budget constraints, skills shortages, and rising data security and compliance demands.

77% plan to increase cloud budgets in the next 12 months, up from **60%** in 2023 – driven by rapid digitalisation and market disruption.

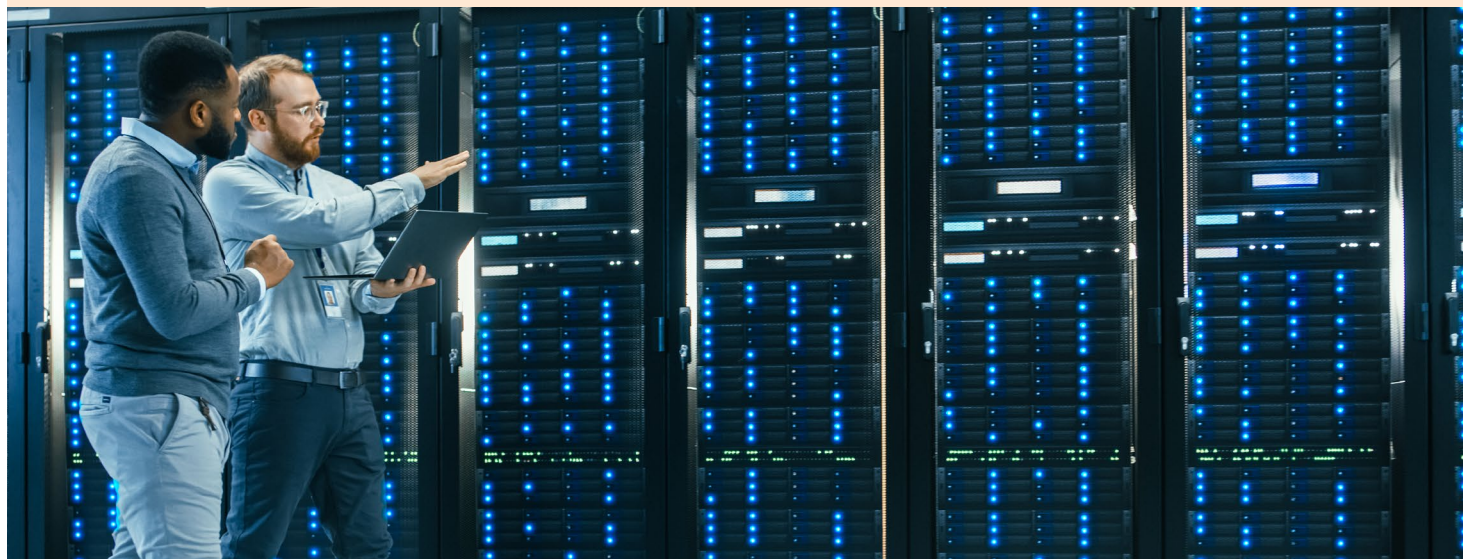
Risk mitigation is the primary driver for changing or modernising cloud infrastructure, followed by AI enablement and cost optimisation.



Cloud has become the backbone of digital transformation in Switzerland. The priority now is to optimise, govern, and secure cloud environments so organisations can innovate confidently and accelerate their AI journey.

Claudius Meyer

Partner, Cloud, Data and AI, PwC Switzerland

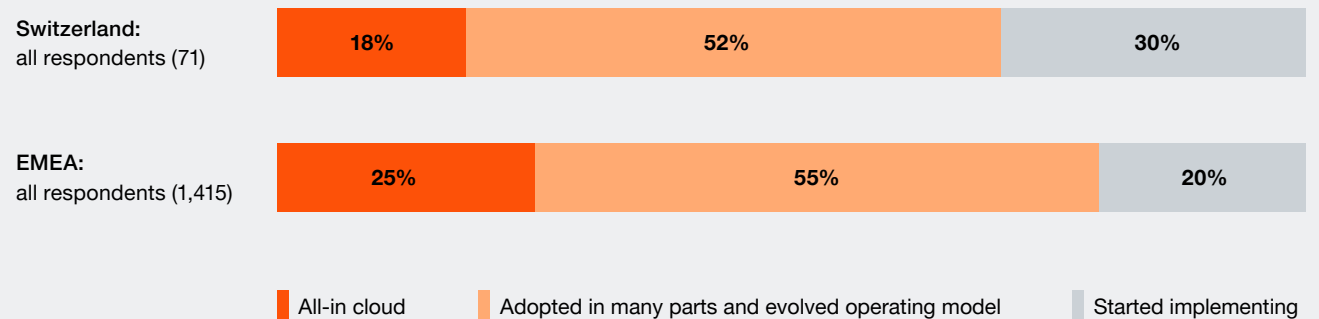


Maturity is gaining serious traction

Cloud maturity in Switzerland has progressed substantially since 2023. All surveyed organisations are now using cloud, either having implemented it in parts of the business or scaled it more broadly. This marks a major shift from 2023, when almost a quarter of respondents stated they were “not currently using cloud but exploring it”.

In 2025, 52% of organisations in Switzerland report that they have adopted cloud in many parts of the business and evolved their operating model. Another 30% have started implementing cloud in some areas. 18% now describe themselves as all-in on cloud, having scaled cloud across the organisation, a marked increase from just 7% in 2023. These results demonstrate that the exploration phase has passed and that cloud has become firmly embedded across the Swiss market.

Which of the following best describes your organisation use of cloud?



Overall, Switzerland has significantly improved its cloud maturity and has largely closed the gap with the broader EMEA region, where a similar share of organisations now report medium or high maturity.

This step-change reflects a clear shift from adoption to optimisation: Swiss organisations are modernising architectures, strengthening cost controls, and integrating cloud more deeply into their digital and business strategies.

Barriers and challenges

Internal barriers continue to limit the value Swiss organisations can extract from their cloud strategies. Budget and investment constraints remain the most frequently cited obstacle, mentioned by 38% of respondents. This is almost unchanged from 40% in 2023.

Skills shortages have become a far more acute issue, rising to 35% from 26% in 2023. As more mission-critical workloads move to the cloud, demand for specialised cloud, security, and architecture talent is intensifying. The fast pace of technological change further complicates hiring and upskilling, making it difficult for organisations to build the capabilities they need.

Data security and compliance concerns have also increased, cited by 34% of respondents compared with 24% in 2023. This rise likely reflects heightened geopolitical uncertainty and evolving regulatory requirements, including lawful-access debates and concerns related to frameworks such as the CLOUD Act.

Which, if any, are the biggest internal barriers to your organisation achieving measurable value from your cloud strategy? (select top three)



Looking ahead, technology disruption is emerging as the next major pressure point: 51% of organisations plan to address it in the next 12 months. Rapid shifts in architectures, AI capabilities, and digital innovation are becoming strategic challenges. With rising pressure to unlock innovation and limited investment budgets, the growing focus on FinOps focus is undeniable.

Taken together, these hurdles explain why many organisations are reassessing their operating models and governance structures – and why reliance on managed cloud services is expected to grow as companies seek to bridge skills gaps, ensure ongoing optimisation, and stay compliant with evolving security and regulatory demands.



Swiss organisations are realising that cloud value depends less on technology choices and more on having the right skills, operating models, and governance to keep pace with rapid change.

Claudius Meyer

Partner, Cloud, Data and AI, PwC Switzerland



Cloud investment continues to accelerate

Despite the internal challenges Swiss organisations face, the investment outlook remains positive.

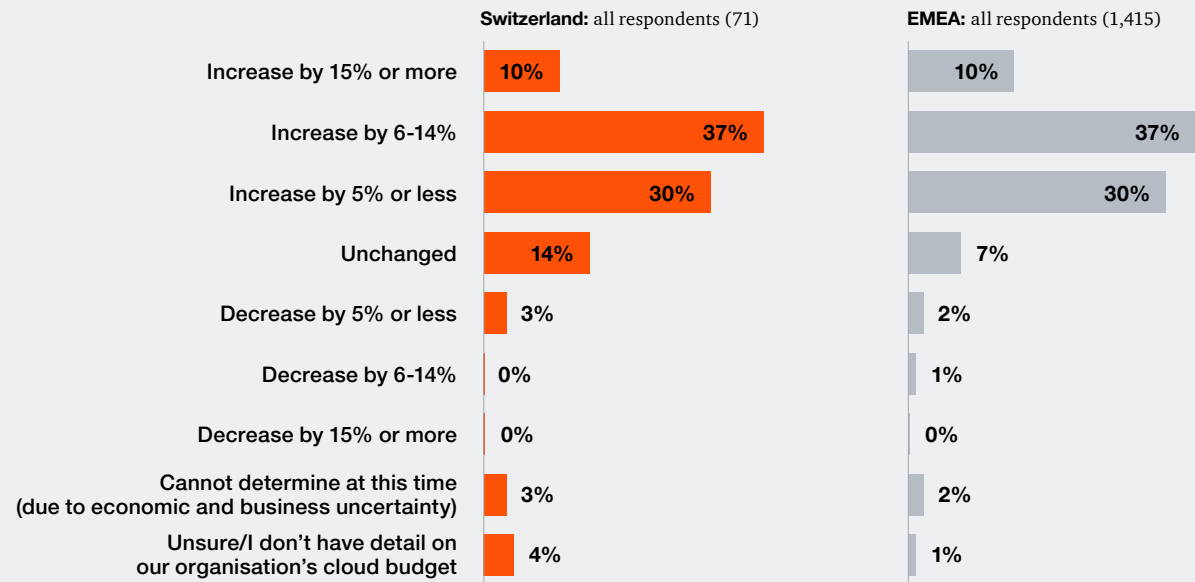
77%

will increase their cloud budget over the next 12 months

This indicates that cloud continues to be viewed as a strategic enabler rather than an area for cost reduction.

At the same time, many organisations still struggle to fully translate cloud spending into measurable returns. As in EMEA, stronger cost governance and FinOps discipline will be key to ensuring that increased spend aligns with business value and that cloud investments support long-term efficiency and innovation goals.

How is your organisation's cloud budget changing over the next 12 months?



Cloud is taking over an increasingly large share of overall IT budgets. Implementing the right controls through FinOps will help organisations turn higher spend into real value and allocate costs to customers with greater precision.

Rejhan Fazlic

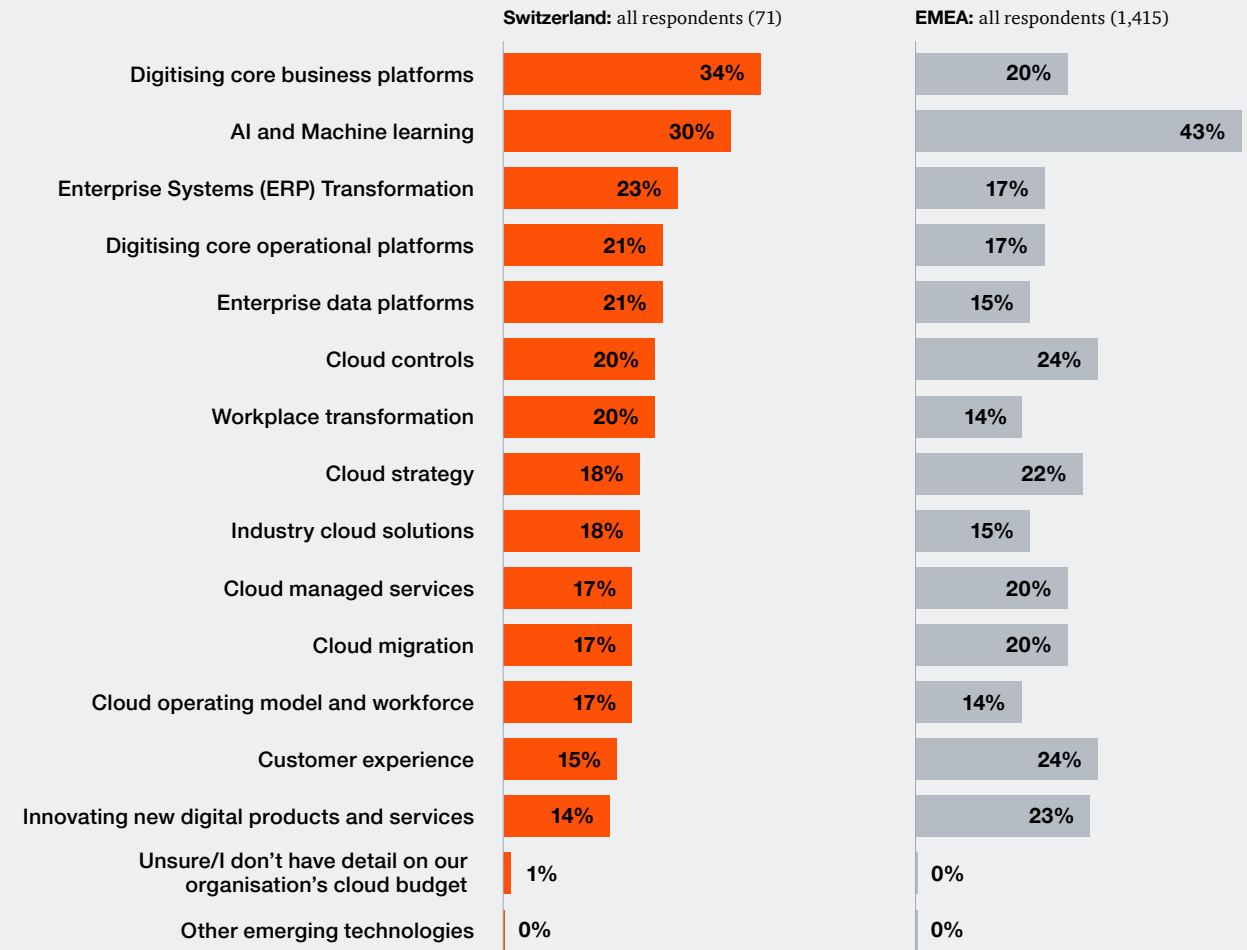
Partner, Technology & Strategy Transformation, PwC Switzerland

Investment priorities

Swiss organisations show a more balanced investment profile compared with the overall EMEA region. While AI and machine learning is the clear top priority across EMEA (43%), Switzerland places digitising core business platforms (34%) slightly ahead of AI and machine learning (30%). This suggests that many Swiss organisations are still strengthening foundational systems before scaling advanced AI capabilities.

Interestingly, despite investing proportionally less in AI than their EMEA peers, Swiss leaders nevertheless expect AI to deliver the greatest future impact on their organisations. This gap between expected value and current investment indicates that many companies are preparing the groundwork by modernising platforms, improving data structures, and enhancing cloud environments before accelerating AI deployment.

Which of the following cloud investments is your organisation prioritising in the next 12 months? (select top three)

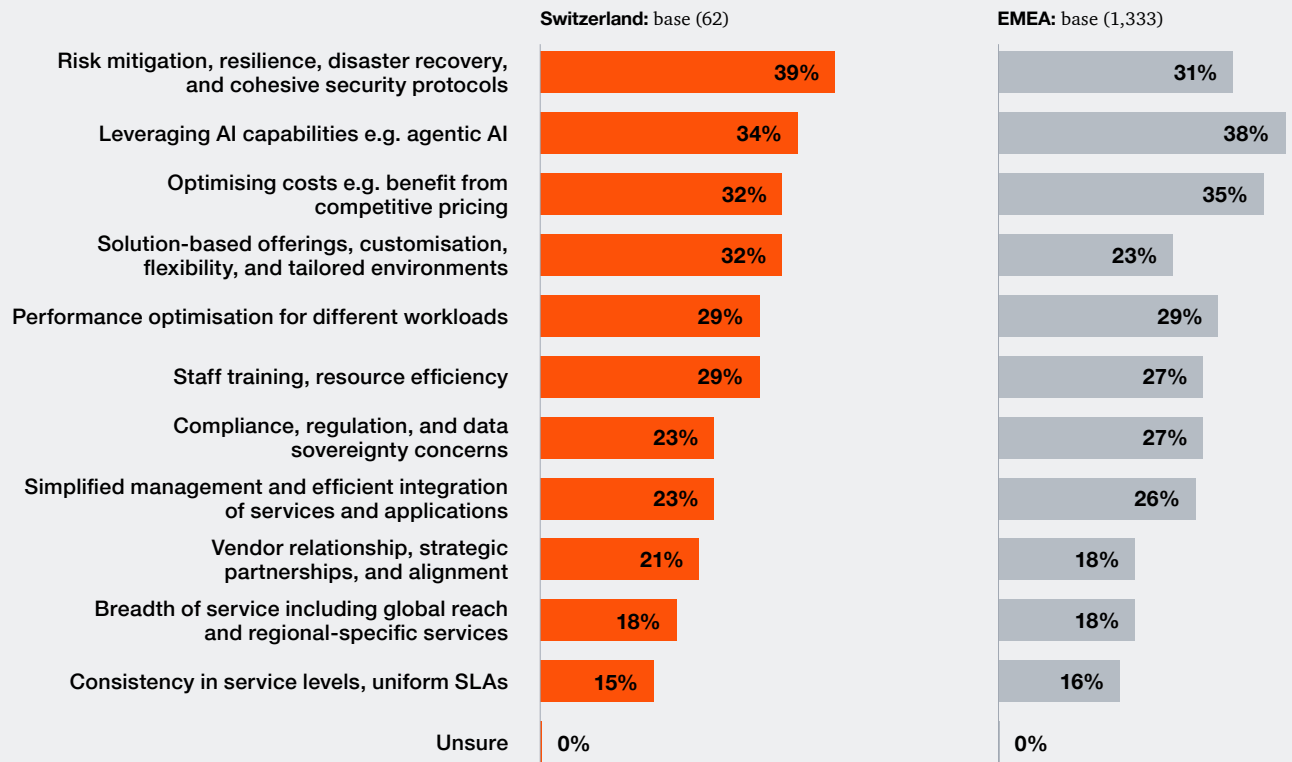


Drivers for cloud infrastructure change

For Swiss organisations, the primary driver for changing or modernising cloud infrastructure is risk mitigation, resilience, disaster recovery, and cohesive security protocols, cited by 39% of respondents. This confirms a long-standing priority in Switzerland: ensuring operational continuity and protecting sensitive data in an increasingly volatile geopolitical and regulatory environment. Unlike in the broader EMEA region, where leveraging AI capabilities is the top reason for change, risk considerations remain the leading motivator in Switzerland.

AI capabilities, however, have become the second-most important reason for cloud infrastructure change. This aligns with what we consistently hear in client conversations: organisations are exploring how to harness AI and agentic AI capabilities without compromising data security. As AI use cases become more advanced and data-intensive, many companies are reviewing their cloud foundations to ensure they can deploy these capabilities safely and at scale.

What are the main reasons your organisation is changing, or planning to change, your cloud infrastructure? (select top three)



Base: Respondents whose organisations are changing types of cloud infrastructure

Cost optimisation ranks third, slightly lower than in EMEA, where it is the second most important priority. Nevertheless, the Swiss results underline a continued need for stronger FinOps practices to manage cloud spend effectively and ensure that investments deliver measurable business value.

Across the top priorities – risk mitigation, AI enablement, and cost optimisation – the message is consistent: Swiss organisations recognise that achieving these goals requires targeted cloud infrastructure improvements, whether through modernised architectures, enhanced security measures, or more efficient operating models.



Risk resilience remains the number one trigger for cloud change in Switzerland. As AI rises, organisations must modernise their foundations and improve data quality, governance, and security.

Urs Küderli

Partner Cybersecurity and Privacy Leader, PwC Switzerland



Risk mitigation is the primary driver for changing or modernising cloud infrastructure, followed by AI enablement and cost optimisation.

Alexandra Burns

Partner, Leader Financial Services Risk Consulting & Internal Audit PwC Switzerland

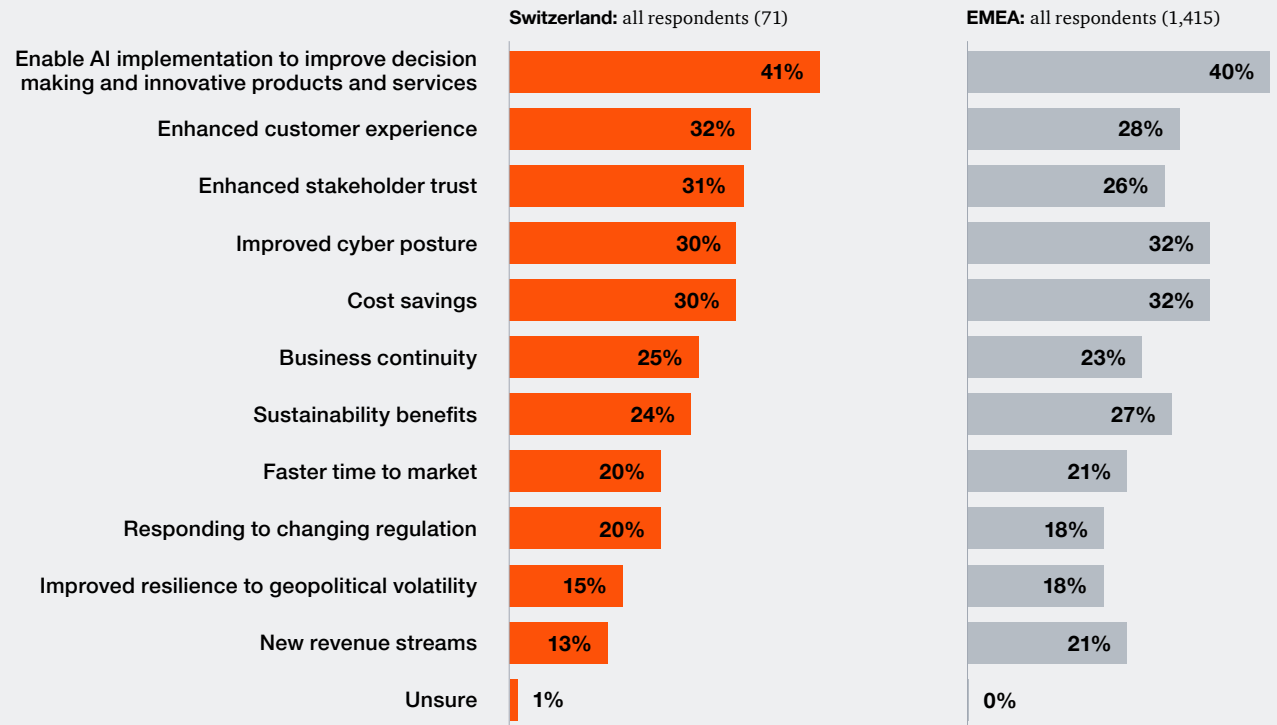
What's next: AI takes centre stage in cloud expectations

AI may not yet be the primary investment focus, but it is the top expected outcome of cloud. 41% of Swiss respondents see AI as key to better decision-making and new products, a clear sign that expectations for AI-driven value creation are rising.

With cloud adoption maturing, Swiss companies are also placing strong emphasis on enhancing customer experience (32%) and strengthening stakeholder trust (31%). As more business processes and customer interactions shift to digital channels, the cloud increasingly serves as the backbone for delivering seamless experiences and maintaining confidence among clients, partners, and regulators.

Improved cyber posture (30%) and cost savings (30%) also feature prominently among expected outcomes, reflecting the continued need to balance innovation with resilience and efficiency.

Which of the following outcomes is your organisation prioritising from your investment in cloud technology over the next 12 months? (select top three)



Swiss organisations see the next phase of cloud investment as the gateway to AI-enabled intelligence, better customer experiences, and more resilient, trusted operations.

Prafull Sharma

Partner, Technology & Strategy Transformation FS, PwC Switzerland



Geopolitics and regulation: the new cloud borders

Geopolitics and regulation are redefining the rules of cloud

46%

of Swiss organisations cite regulation and compliance requirements as the most significant external challenge to extracting measurable value from cloud.

The debate on digital sovereignty is accelerating in Switzerland. Geopolitical tensions and cross-border regulations – including the US CLOUD Act, which allows US law-enforcement authorities in some situations to request access to data worldwide in the context of criminal investigations – are reshaping how organisations think about cloud. Even if such access is rare, protective measures remain essential for Swiss companies.



As digital sovereignty moves to the top of the Swiss agenda, organisations must balance openness with control – navigating cross-border rules, protecting sensitive data, and ensuring trusted, resilient cloud operations.

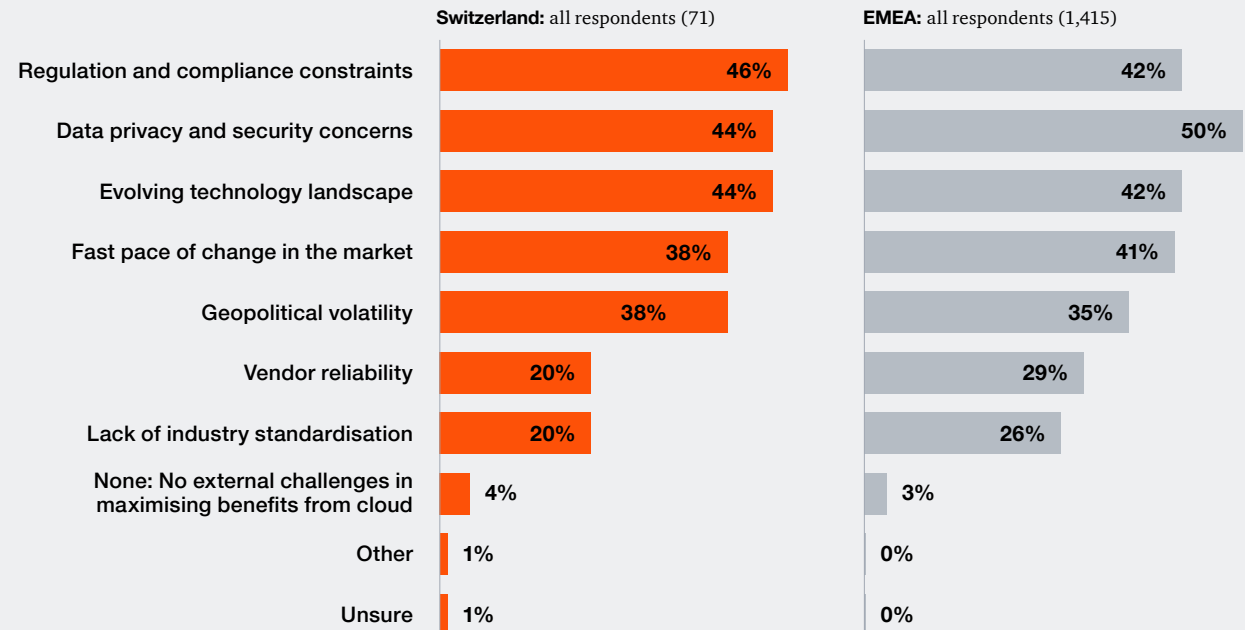
Philipp Rosenauer
Partner, Legal, PwC Switzerland



External challenges: regulation, privacy, and a fast-moving tech landscape

Swiss organisations see regulation and compliance requirements (46%), together with data privacy and security concerns (44%), as the most significant external challenges to realising measurable value from their cloud strategies. This reflects a market environment in which geopolitical developments and lawful-access discussions have become central to cloud adoption. Trust in cloud technologies increasingly depends on how clearly companies can navigate cross-border regulations, protect sensitive data, and ensure that their cloud environments remain compliant across jurisdictions.

Which, if any, are the biggest external challenges to your organisation achieving measurable value from your cloud strategy? (select top three)



At the same time, the rapidly evolving technology landscape (44%) adds pressure: new capabilities emerge faster than many organisations can adapt their governance models, skills, and architectures. This combination of regulatory complexity, heightened security expectations, and constant technological change forms the key external barrier that Swiss leaders must address to translate cloud investments into business impact.

Redrawing the cloud map

Geopolitical tensions and new regulations are reshaping how data is stored, processed, and secured. Governments are mandating localisation and “sovereignty-by-design” models that coexist with global ecosystems – so organisations can operate securely within regulated environments and maintain control over sensitive data.

Many Swiss organisations are now setting their own sovereignty-by-design benchmarks. Often, the starting point is data classification (e.g. public, internal, confidential, secret) and mapping it to different deployment locations, such as the cloud levels defined by the Swiss Government Cloud (see page 27). This mapping provides clarity on when public cloud services can be used and in which situations additional measures are needed.

The Swiss Government Cloud illustrates Switzerland’s drive to combine global cloud ecosystems with local governance, control, and data sovereignty – enabling both innovation and regulatory alignment under one umbrella.



With the Swiss Government Cloud, organisations gain a sovereignty-by-design model that balances openness with strict governance, giving them confidence to run sensitive workloads securely.

Philipp Roth

Partner, Government & Public Sector Leader, PwC Switzerland



Navigating a maze of regulation

Regulatory fragmentation is accelerating. From GDPR, NIS2, DORA, and the Cyber Resilience Act to the EU AI Act and emerging digital sovereignty frameworks, organisations face complex compliance obligations, differing enforcement practices, and rising costs. While NIS2 applies to critical infrastructure and DORA targets financial services, large organisations across all sectors can apply the underlying principles to strengthen their overall resilience. For global companies, the implications are strategic: governance and risk management must evolve in step with innovation ambitions. This dynamic also affects Swiss organisations, many of which are closely integrated with EU markets and therefore need to ensure that their cloud environments remain compatible with multiple regulatory requirements.



Cybersecurity is firmly embedded in cloud strategies. But many organisations still underestimate the speed and scale of technology disruption, making strong cloud assurance more critical than ever.

Narcisse Vieira

Partner, Cloud Assurance, PwC Switzerland

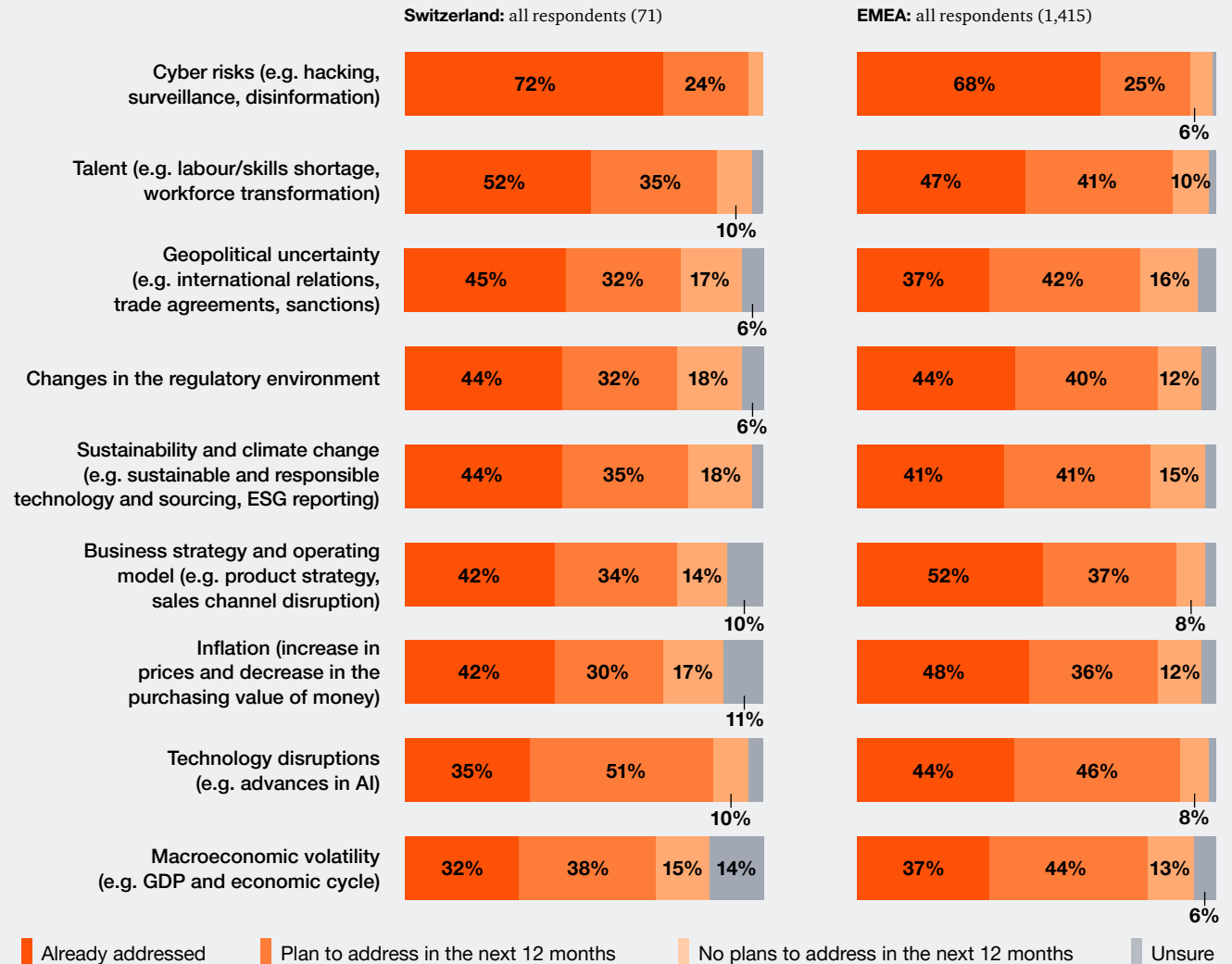


Security first – and a clear view of what comes next

Cybersecurity remains the most established pillar of Swiss cloud strategies. 72% of organisations have already addressed cyber risks, above the EMEA average of 68%. An additional 24% in Switzerland plan to do so in the next 12 months. This strong focus reflects the high level of maturity Swiss organisations have built over recent years, as well as the continued pressure to safeguard critical workloads in an increasingly complex threat landscape.

Looking ahead, Swiss leaders plan to focus their cloud efforts on a set of broader resilience themes. The top areas they intend to address next include technology disruption, macroeconomic volatility, talent and workforce transformation, sustainability and climate change, and business strategy and operating-model adaptation. Together, these priorities signal where cloud is expected to play a central role in strengthening future readiness.

Which, if any, of the following risks and challenges have been addressed in your organisation's cloud strategy?



As Swiss organisations prepare to address these emerging challenges, the question increasingly becomes how they can do so in a way that strengthens their sovereignty posture and builds lasting trust.



Sovereignty and trust: building resilient cloud strategies

Sovereignty is not only about compliance – it's a strategic essential

75%

of Swiss organisations operate multi-cloud environments to strengthen control, resilience, and regulatory trust while leveraging the best capabilities of each provider.

Digital sovereignty refers to the ability of public and private organisations to retain control over their digital infrastructure and data. It ensures they have the flexibility to operate across multiple cloud environments while using advanced technologies to safeguard and manage their data according to local regulations and operational needs.

The survey shows that 75% of Swiss organisations operate in a multi-cloud environment, compared with 25% using a single-cloud setup. This aligns with what we observe in practice: many organisations work with more than one cloud provider, but typically with a primary hyperscaler at the centre of their architecture, while only a small number run a truly independent multi-cloud setup.

“

Swiss companies have moved to the cloud. The challenge now is to stabilise the environment, ensure sovereignty and operate with excellence. Optimisation and mature multi-cloud models will be key to unlocking the next wave of value.

Claudius Meyer

Partner, Cloud, Data and AI, PwC Switzerland



Swiss organisations are diversifying their cloud environments to strengthen trust, resilience, and control. They are balancing flexibility with the need to meet regulatory, operational, and sovereignty requirements.

Narcisse Vieira

Partner, Cloud Assurance, PwC Switzerland



What sovereign cloud entails

Sovereign cloud models ensure that cloud services – from data storage and processing to applications – are delivered in a way that meets national regulatory requirements and organisational governance standards. These solutions define where data resides, how it is handled, and who has access, allowing organisations to balance regulatory alignment, operational flexibility and innovation.

Different approaches offer varying degrees of autonomy and agility, and all have become integral to cloud strategy discussions. Moving entirely to private cloud may appear to be the simplest path to full control, but it comes with trade-offs: organisations risk losing the pace of innovation and the economies of scale provided by global hyperscalers. Sovereign public-cloud solutions aim to close this gap by combining local governance with the technological advancements of international platforms.



Where is my data stored? This has become the new trust question, one that matters as much to customers as it does to governments.

Claudius Meyer

Partner, Cloud, Data and AI, PwC Switzerland



The Swiss context

In Switzerland, sovereignty in the cloud is increasingly shaped by the tiered model of the Swiss Government Cloud, which differentiates between levels of control, data handling, and operational requirements. The following cloud levels reflect how organisations can balance sovereignty, flexibility, and innovation within Swiss regulatory requirements:

Public Cloud Standard (Level I)

Commercial hyperscaler services (e.g., Microsoft Azure, Google Cloud, Oracle Cloud, AWS) with full functionality and operated globally. These services allow organisations to scale flexibly but require additional measures if sensitive data exist or sovereignty requirements apply.

Public Cloud Switzerland (Level II)

Public cloud with data stored and processed in Switzerland, or safeguarded by additional technical and organisational measures.

Private Cloud (Level III)

Dedicated cloud environments operated exclusively for a single organisation by a Swiss provider, with resources logically separated from other tenants. This setup offers greater control and meets stricter sovereignty or compliance needs.

Secure Private Cloud (Level IV)

Highly protected environments for workloads subject to special legal requirements (e.g., classified information, highly sensitive operations); currently specific to governmental use cases where the infrastructure is provided by a government-owned entity.

No Cloud/On-premises

Workloads that remain on traditional infrastructure due to legal, operational, or legacy constraints.



Sovereign cloud is about maintaining controls and stability. It ensures that data location, protection, and governance meet national requirements despite continuous geopolitical change, without giving up the flexibility and innovation of modern cloud services.

Chris Girling

Partner, Cybersecurity and Privacy, PwC Switzerland



Compliance as a catalyst for innovation

The EU AI Act places cloud-based AI solutions directly under regulatory scrutiny, making governance a core priority. Compliance and innovation are no longer trade-offs; they must progress in parallel. This is also relevant for Swiss companies, many of which operate across EU markets or provide services to EU clients.

The fact that three out of four enterprises have adopted a multi-cloud strategy shows how organisations are maximising innovation potential while sourcing services with the best cost-benefit ratio from each provider. This approach also intensifies competition among vendors, enabling organisations to secure stronger discounts and more favourable commercial terms.



Trusted partnerships and ecosystems

Trusted partnerships are emerging as a critical enabler. Hyperscalers are building new sovereign solutions and dedicating resources (including Chief Security Officers), investing in local capabilities and offering data-residency and sovereignty-supporting controls. At the same time, Swiss providers and managed service partners play a critical role by tailoring cloud environments to specific legal, operational, and industry requirements, strengthening local trust. The result is an ecosystem where clients benefit from active competition and massive investment, with flexibility, multi-cloud models, and new partnership approaches giving them more choice than ever.



Ethics and governance

As organisations increasingly look to the cloud to enable AI, ethical and governance considerations are gaining urgency. Ensuring responsible use of AI, protecting sensitive data, and aligning with national and international standards are becoming central to building long-term trust in cloud ecosystems. Swiss organisations increasingly recognise that sovereignty and trust go hand in hand: a cloud strategy that provides transparency, control, and clear governance is essential not only for compliance, but also for enabling AI-driven innovation in a safe and accountable way.



Trust is becoming a decisive advantage. Whether in sovereign cloud or responsible AI, organisations are weaving transparency and ethical principles into their technology agendas – the foundations of a truly trusted transformation.

Claudius Meyer

Partner, Cloud, Data and AI, PwC Switzerland





Agentic AI: the next frontier of cloud intelligence

AI is no longer an add-on – it's the engine of cloud innovation

Agentic AI adoption is at an early stage: only

15%

of Swiss organisations are implementing and scaling, suggesting that the next stage of maturity is just beginning.

Agentic AI moves beyond traditional machine learning by enabling systems to act autonomously, adapt to new information, and execute complex tasks with minimal human intervention. While concrete use cases are still emerging, the topic is already highly visible across Swiss organisations.

The Swiss results show that 72% of organisations are currently piloting or exploring agentic AI, signalling strong momentum but also that most companies remain early in their journey. Only 15%, compared with 29% in EMEA, are already implementing and scaling these capabilities.

How would you describe your organisation's use of Agentic AI?



This suggests that the next stage of AI-driven maturity is just beginning and is likely to become a major differentiator for those who move quickly and implement effectively. We observe in Switzerland that the start of the AI implementation journey is often triggered by needs arising in business operations, not necessarily within IT departments. However, IT infrastructure must be ready to meet the increasing and disruptive demands from the business, which in turn underscores the need for mature cloud operations.

In contrast, 13% have not yet started to consider agentic AI, placing them at risk of falling behind the clear trend toward advanced AI capabilities in both Switzerland and the wider EMEA region. As agentic AI gains traction, these organisations may face increasing pressure to catch up in order to maintain competitiveness.



“

To realise the full potential of AI, Swiss organisations still need to strengthen their data foundations. Those embarking on the AI journey should ensure that their architecture is purpose-designed early and built for scale.

Joscha Milinski

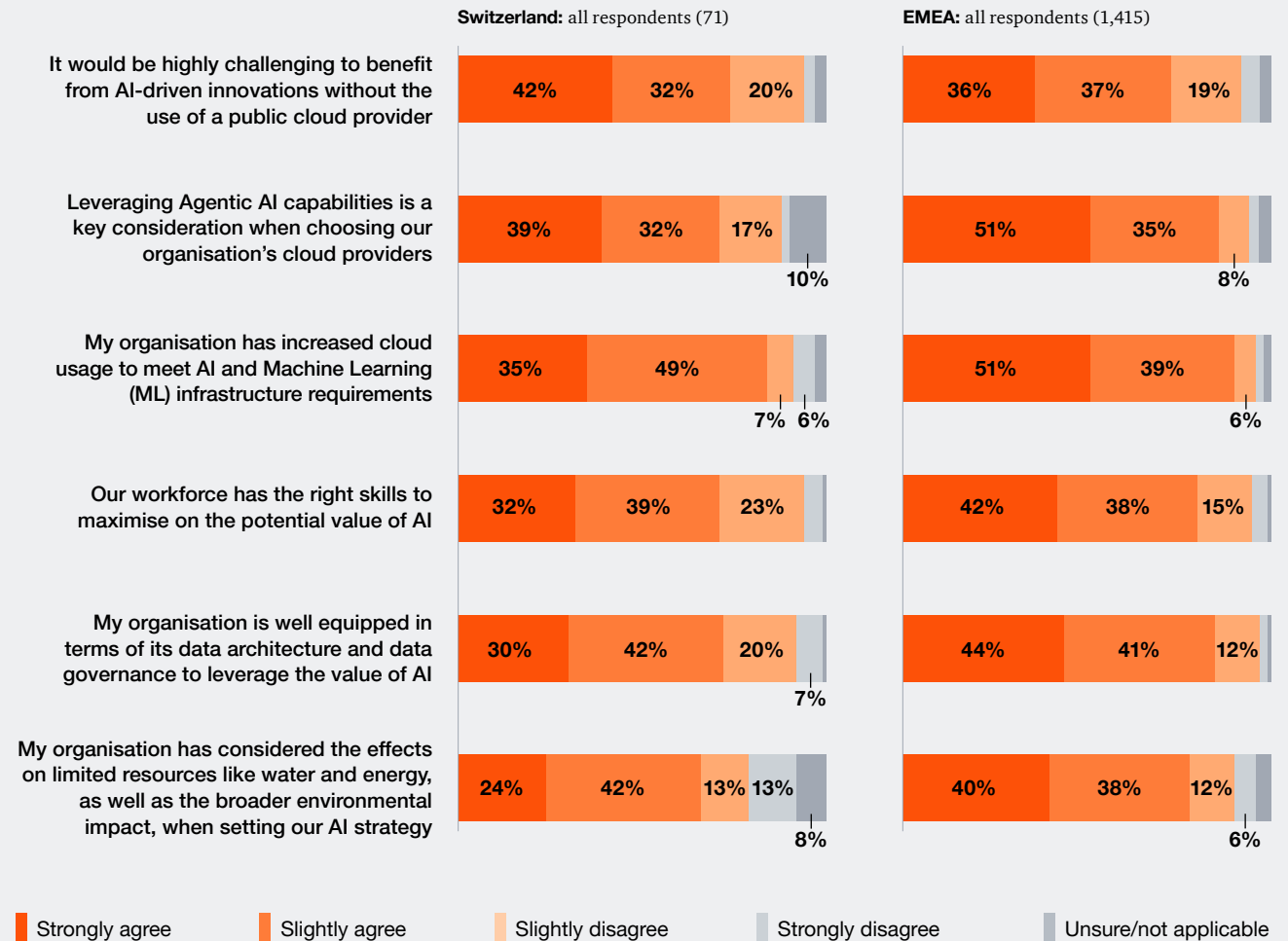
Partner, Cloud, Data and AI, PwC Switzerland

AI readiness: skills and data architecture remain critical gaps

While Swiss organisations are increasingly engaging with AI, many still feel insufficiently prepared to fully capture its potential. Only 30% agree that their organisation is well equipped with the necessary data governance and architecture, noticeably lower than the 44% reported across EMEA. Similarly, just 32% of Swiss respondents believe their workforce has the right skills to maximise AI's value, compared with 42% in EMEA.

These results point to a clear readiness gap: even as investment and interest in AI accelerate, skills, data structures, and governance frameworks remain behind where they need to be. Strengthening these foundations will be essential for Switzerland to move from early experimentation toward scalable, high-value AI adoption that delivers measurable business impact.

To what extent do you agree or disagree with the following statements about your organisations use of Artificial Intelligence (AI)?





Cloud economics: managing the cost of innovation

The promise of cloud is agility – but managing costs is the real test of value.

FinOps is becoming essential:

77%

of Swiss organisations already use or plan to use FinOps, underlining the need for systematic cloud cost governance.

Cloud delivers agility and speed, but its very ease of scaling can also lead to rising and unpredictable costs. Many organisations find it challenging to balance flexibility with the financial discipline needed to maintain a strong cloud business case. Without structured governance, cloud spend can quickly drift away from strategic priorities.

This is where FinOps comes in. FinOps provides a framework for embedding financial accountability into cloud operations.



Cloud delivers speed, but without FinOps discipline its costs can drift quickly. Financial accountability turns cloud spend from a volatile expense into a value-driven investment.

Rejhan Fazlic

Partner, Technology & Strategy Transformation, PwC Switzerland

It strengthens collaboration between engineering, finance, procurement, and business teams, ensuring that cloud spending is actively managed and tied to measurable outcomes. When implemented well, it turns cloud costs from a fluctuating expense into a predictable, value-driven investment.

FinOps adoption: growing discipline, varied maturity

FinOps is gaining strong momentum in Switzerland. 38% of organisations have already adopted FinOps practices, and another 39% are piloting or planning to apply them – similar to the overall EMEA trend. This is a clear sign that systematic cloud cost management has become a priority. Only a minority (15%) have not yet recognised the need for FinOps.

However, adoption levels vary considerably. While some organisations are integrating FinOps across engineering, finance, and operations, others are focusing on specific capabilities such as cost visibility or optimisation. This spread reflects a broader reality: establishing a full FinOps practice requires time, coordination, and sustained effort. As cloud usage scales, building this discipline will be essential to ensure costs remain transparent, controlled, and aligned with business value.

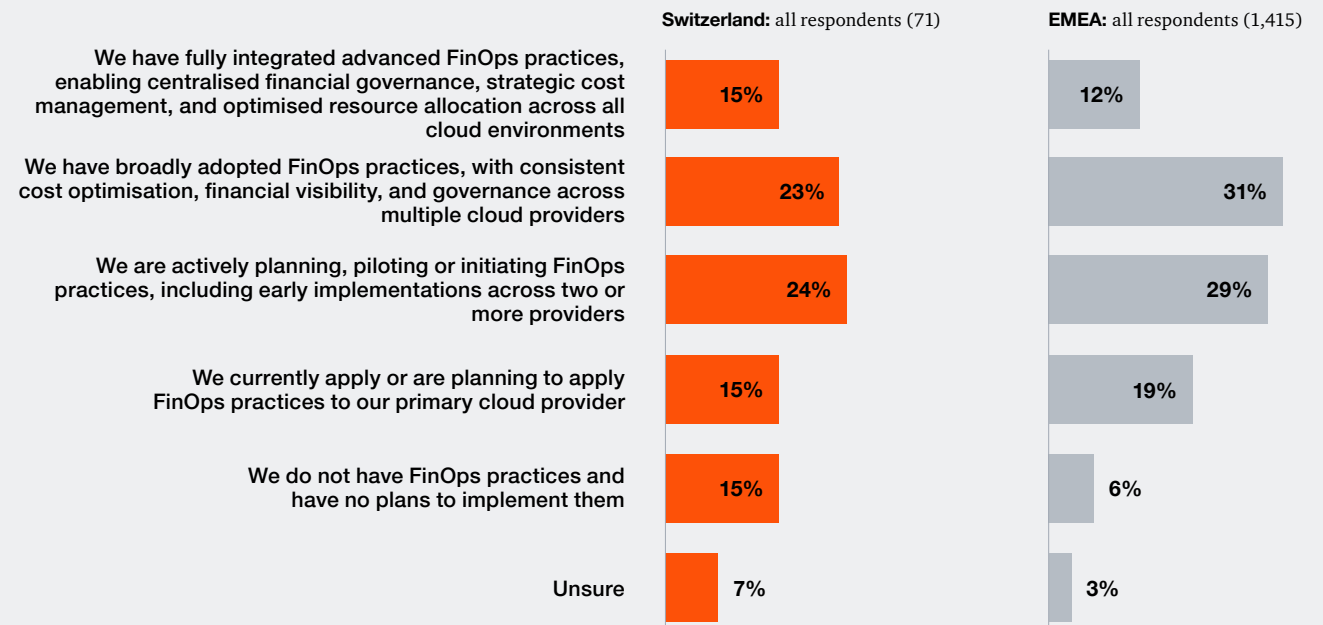


FinOps is gaining traction in Switzerland, but maturity still lags cloud adoption. As workloads scale, structured cost governance will be essential to keep spending transparent, controlled, and tied to real business impact.

Claudius Meyer

Partner, Cloud, Data and AI, PwC Switzerland

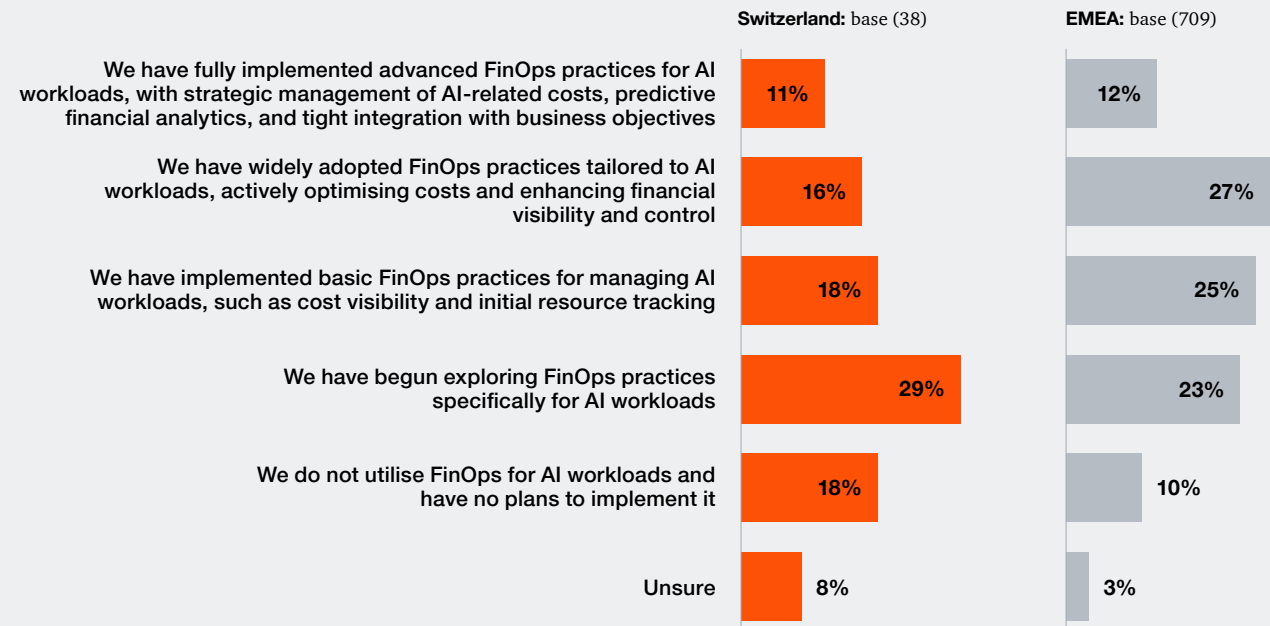
Which of the following statements best describes your organisation's current adoption of FinOps practices?



FinOps for AI workloads: early stages of adoption

While FinOps has gained traction for general cloud spending, its adoption for AI workloads is still at an early stage in Switzerland. Only about one in four organisations have already implemented FinOps practices tailored to AI, and almost half are still only exploring or applying basic approaches such as initial cost tracking and visibility. The results suggest that FinOps for AI is emerging, but not yet widespread, a natural consequence of AI's rapid uptake and the new cost models associated with large-scale, data-intensive workloads. As AI usage grows, building dedicated FinOps capabilities will become essential for ensuring transparency, control and long-term financial sustainability.

Which of the following statements best describes your organisation's current adoption of FinOps practices for AI workloads?



Base: Respondents in tech roles



AI workloads are increasing, but we are still at an early stage of FinOps for managing them. Few concrete use cases and only emerging frameworks underline how new this field still is.

Rejhan Fazlic

Partner, Technology & Strategy Transformation, PwC Switzerland



**Conclusion: embracing
the new age of cloud**



Swiss organisations have significantly advanced their cloud maturity over the past two years, closing much of the gap with the broader EMEA region. This progress comes at a time when sovereignty, regulatory alignment, and risk awareness are becoming central to cloud strategy, areas where Switzerland traditionally holds high expectations for data privacy, control, and compliance.

Although AI is not yet the primary focus of investment, expectations for its impact are substantial. AI will shape the next phase of cloud-driven transformation, but most organisations are still building the foundations required to deploy it safely and at scale.

The path ahead will require Swiss organisations to balance resilience, flexibility, and trust, and to develop the competencies needed to navigate sovereignty requirements, manage complex architectures, and unlock AI responsibly. By treating compliance and data privacy not as constraints but as enablers of innovation, Swiss organisations can strengthen their position and compete effectively in an increasingly international market.

To capture the full value of cloud and AI, Swiss organisations should now take the next step: strengthen the data foundations, modernise architecture, and build the capabilities needed to operate with sovereignty, trust, and efficiency. Those who start now – and do so deliberately – will be best positioned to turn compliance into an advantage, accelerate innovation and compete with confidence in a rapidly evolving digital landscape.

Are you ready to embrace the new age of cloud?

Contacts



Claudius Meyer
Partner, Cloud, Data and AI
PwC Switzerland
+41 58 792 18 84
claudius.meyer@pwc.ch



Alexandra Burns
Partner, Leader Financial Services
Risk Consulting & Internal Audit
PwC Switzerland



Philipp Roth
Partner, Government &
Public Sector Leader
PwC Switzerland



Chris Girling
Partner, Cybersecurity and
Privacy
PwC Switzerland



Prafull Sharma
Partner, Technology & Strategy
Transformation FS
PwC Switzerland



Joscha Milinski
Partner, Cloud, Data and AI
PwC Switzerland



Rejhan Fazlic
Partner, Technology &
Strategy Transformation
PwC Switzerland



Narcisse Vieira
Partner, Cloud Assurance
PwC Switzerland



Urs Kuederli
Partner, Cybersecurity and
Privacy Leader
PwC Switzerland



Philipp Rosenauer
Partner, Legal,
PwC Switzerland

Thank you to our authors and contributors:

Julia Knysak-Müller
Manager Cloud, Data and AI, PwC Switzerland

Markus Iten
Senior Manager, Cloud, Data and AI, PwC Switzerland

