Infrastructure Modernisation Survey

2025

Contents

Foreword

In an ever-changing digital world, businesses face a constant push to adapt, grow, and remain competitive. Cloud transformation has become an essential part of this evolution, offering organisations the tools to innovate, scale effectively, and rapidly respond to shifting demands. But cloud transformation isn't a destination, it's an ongoing journey. A journey that continually changes, empowering organisations to remain agile in an unpredictable world

In today's rapidly shifting digital landscape, choosing the right cloud infrastructure helps you to future-proof your business, enabling you to thrive amidst continuous change, and making infrastructure resilient to a growing range of cybersecurity threats.

Since our inaugural Ekco Infrastructure Modernisation Survey in 2022, digital transformation has only accelerated. Today, an overwhelming 88% of organisations have either completed or are actively engaged in cloud infrastructure initiatives. The shift towards hybrid cloud, now at 68% adoption, demonstrates a maturing approach - organisations are combining the best aspects of public and private clouds with on-premises solutions, driven by successful experiences in earlier migrations.

Yet, as cloud adoption grows, so does its complexity - and the more complex the environment, the tougher it becomes to secure effectively. As a result, security concerns have intensified with 81% of IT leaders expressing concerns over their infrastructure. Most notably, AI-driven security threats have overtaken traditional data breaches as the primary cloud security challenge. This development marks a shift in the cybersecurity landscape, with organisations recognising the need for enhanced monitoring, deeper visibility into potential vulnerabilities, and robust preventative measures.

Compounding these challenges is a significant skills gap: just 27% of organisations feel they have the internal expertise needed to harness cloud technologies fully. This gap is prompting increased collaboration with Managed Service Providers (MSPs). Notably, cloud projects supported by MSPs are 6.6% more likely to achieve their objectives, underscoring the tangible benefits of external expertise in navigating cloud complexities.

Our 2025 survey delves deep into these trends, complemented by expert insights and actionable advice designed to help your business leverage cloud and AI integration strategically. Our aim is clear: to empower you with the knowledge required to confidently optimise your infrastructure, enhance security, and continue your journey of continuous improvement and growth.

We hope this report guides you effectively as you future-proof your organisation, making your journey in the cloud both secure and transformative.

Carla Mendy
COO at Ekco

88%
of organisations have either completed or are actively engaged in cloud infrastructure initiatives

68%
hybrid cloud adoption, demonstrates a maturing approach

81%
of IT leaders expressing concerns over their infrastructure

27%
of organisations feel they have the internal expertise needed to harness cloud technologies fully

Key Findings

70% IT decision-makers using on-premises infrastructure who think they could save money by moving to the cloud.

88% Organisations which have recently completed a cloud infrastructure project or are planning one.

82% Organisations which say moving to the cloud helps create a more agile organisational culture beyond infrastructure improvements.

54% IT decision-makers who lack complete visibility into their cloud costs, highlighting a critical management challenge.

59% IT decision makers who now identify AI attacks as the top cloud security challenge, overtaking data breaches for the first time.

62.3% Organisations which say legacy technology is holding them back, especially those relying entirely on-premises.

87% Cloud infrastructure projects which achieve almost all or all their initial objectives, showing strong overall success rates.

68% Organisations which now adopt hybrid cloud solutions, significantly up from 58% in 2022.

81% IT decision-makers who are concerned about the cybersecurity resilience of their cloud infrastructure.

58% IT decision-makers who actively use AI in their organisations, marking significant growth from 46% the previous year.

CHAPTER 1

Motivations for moving to the cloud

As businesses navigate an increasingly digital world, the decisions they make about technology today will shape their resilience and competitiveness tomorrow. Among these decisions, cloud strategy stands out as the most important infrastructure question.

Get it right, and the rewards are clear: greater scalability, improved efficiency, and accelerated innovation.

Despite years of cloud transformation, many organisations still rely on on-premises systems - and feel limited by them. In fact, according to our research 71% of IT decision-makers say outdated on-premises technology is holding their organisation back, and 70% believe migrating to the cloud could reduce costs.

But what's driving the shift today? And what challenges are organisations facing as they make the move?

Legacy Infrastructure as a Barrier

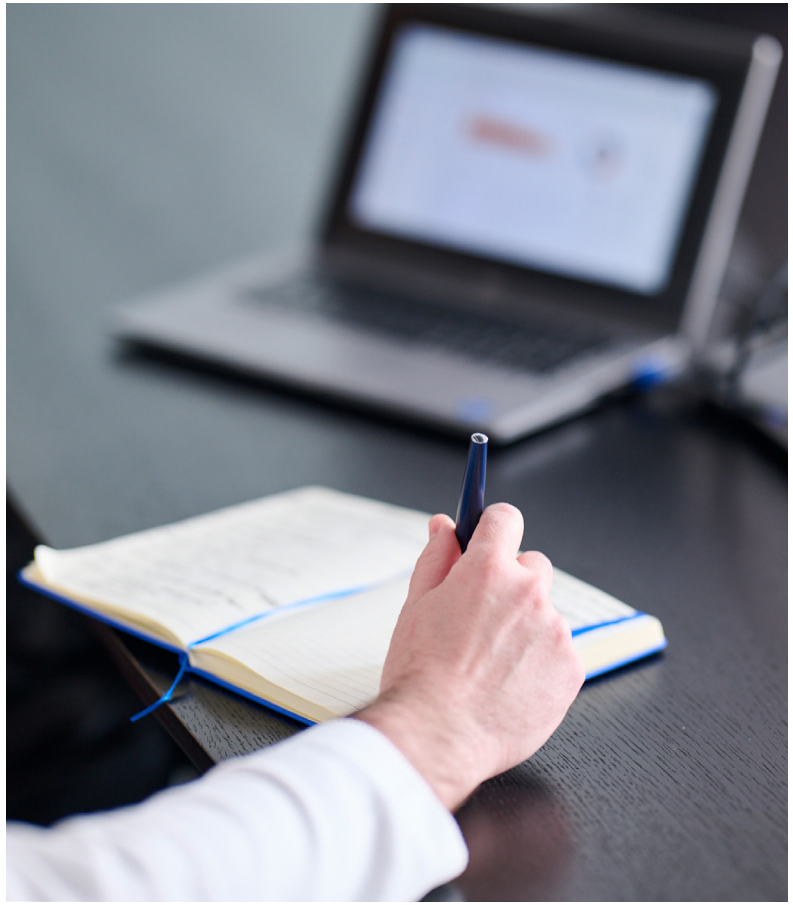
71%

perceive legacy infrastructure as restrictive.

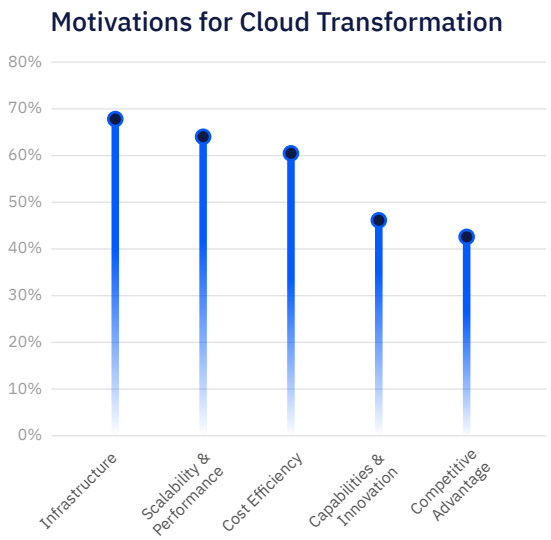
As the pace of innovation accelerates, organisations are increasingly aware of the risks associated with clinging onto aging infrastructure. Many are still running applications that are at - or fast approaching - the end of their support window. This creates a serious security concern: without ongoing vendor updates, these systems are left exposed to vulnerabilities that will go unpatched, potentially putting sensitive data and core operations at risk.

Beyond the security threat, there's also the practical inconvenience of compatibility. Unsupported software may no longer integrate smoothly with modern platforms or tools, creating inefficiencies and limiting future innovation.

Of course, legacy systems may continue to perform their core functions, but they can quietly limit an organisation's ability to take full advantage of modern technologies or integrations. It's little wonder, then, that 98% of organisations are now considering a move to the cloud.



Drivers of Cloud Migration



On a more granular level, there's a variety of motivations for cloud transformation – it's not as simple as just replacing aging infrastructure (although this is the biggest motivation). Organisations are also looking to improve the scalability and performance of infrastructure. Cost is a consideration too.

The question then becomes: "Why hasn't everybody moved to the cloud already?" For those businesses that expressed a desire to migrate, the barriers are often complex. Organisational cultures can be rigid, and it's easy to understand the impulse to simply "make do" rather than face the challenges and costs – real or imagined – associated with transferring IT systems. Similarly, many managers simply don't see migration as a priority.

37% **Make do mentality**

46% **Management not prioritising cloud migration**

Common barriers include the "make do" mentality (37%) and management not prioritising cloud migration (46%)

> *"Securing management buy-in is critical. Organisations often stall migration because leadership doesn't see cloud transformation as a strategic priority, which delays realising the full potential of modernisation."*
>
> **Peter Thomas,** *Senior Manager Cloud & Security Architecture at Ekco*

It's crucial that IT decision makers don't lightly dismiss these concerns - they need to be treated as seriously and delicately as the technical challenges of cloud migration. Understanding the beliefs and assumptions behind cloud hesitancy, correcting any misconceptions, and providing clear, easy-to-understand roadmaps for adopting new technologies is an essential starting point to allow businesses to unlock the full potential of cloud.

Overcoming the Skills Gap

Of course, it would be wrong to suggest that cloud migration is always plain sailing. Once the high level barriers are dealt with, organisations need to grapple with sometimes difficult realities. Today, skills shortages are amongst the biggest concerns with only around a quarter of organisations feeling confident that they have the in-house skills to expand their cloud use to the extent they would like, and this, in turn, can contribute to hesitancy among managers and a feeling that it's simply easier to continue using legacy systems.

> *"Most cloud adoption programmes fail because IT underestimates the true benefits beyond simple CapEx versus OpEx calculations. Hidden costs like staff training and vendor lock-in frequently get overlooked, causing unforeseen expenses."*
>
> **Peter Thomas,** *Senior Manager Cloud & Security Architecture at Ekco*

27%

Only 27% of organisations feel they have the skills in-house to grow and expand their use of the cloud.

One answer to overcoming any skills gaps is to leverage the support of external consultants. MSPs provide expertise to help optimise processes for a business's specific needs and simplify the process of migrating data and workflows from on-prem systems to the cloud. It's important that MSPs are adaptable: able to both fully manage cloud environments for companies if required, or simply to support and supplement internal capabilities.

Strategic vs. Tactical Cloud Adoption

Something that's often missed in discussions of the topic is that cloud migration can take many different forms. Each organisation will have a different approach and a different set of incentives. Broadly speaking, this will fall into one of two categories: tactical or strategic cloud adoption.

Tactical adoption refers to businesses undertaking cloud projects to address immediate needs, usually a short-term, specific project, or to target one clearly defined operational issue. This isn't a bad thing per se, but it can mean companies miss out on long-term benefits. In some cases, it can result in a patchwork of cloud platforms with limited interoperability, exacerbating the short-term problems each project was designed to solve and creating new ones.

A strategic approach considers broader considerations, allowing businesses to ensure the benefits of cloud adoption are felt across a range of operational areas. Comprehensive planning allows leadership teams to see how a larger cloud migration project – whether fully public or hybrid – can resolve a wide range of immediate problems and introduce efficiencies in the long term. It's the digital equivalent of choosing prevention rather than a short-term cure.

Five Tips for Getting Management Buy-In

1. Lead with business outcomes

Position cloud transformation as a strategic enabler – link it to goals like cost control, operational agility, and faster time to innovation.

2. Highlight the risk of falling behind

Rather than simply focusing on threats, show how relying on outdated systems can quietly erode competitive edge – from slower delivery to missed innovation opportunities.

3. Use trusted partners to bridge the gap

Highlight how engaging an experienced MSP partner can reduce risk, fill internal skills gaps, and ensure a smoother, lower-stress transition to the cloud.

4. Tell the success stories

Share relevant industry examples that show real-world value – especially when cloud adoption has led to measurable improvements.

5. Present a phased, low-risk roadmap

Propose a pragmatic plan that starts small, scales incrementally, and builds confidence at every stage – making success easy to see.

CHAPTER 2

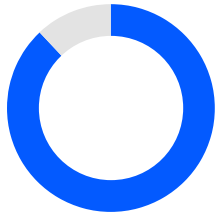
Success metrics around cloud modernisation

Cloud modernisation is more than just a technical upgrade - it's a strategic investment. But how do organisations know if their efforts are paying off?

Our research suggests many are seeing strong returns, with the vast majority of cloud infrastructure projects delivering against their goals. But only a third met every objective, signalling clear opportunities to improve how success is defined, measured and delivered.

So how are businesses tracking progress? What outcomes are they seeing in practice? And where could the right support - such as from a Managed Service Provider - help them go even further?

Defining and Measuring Success



88%

of organisations have recently completed a cloud infrastructure project or are planning one, and of those **87%** claim they achieved all or almost all of their objectives

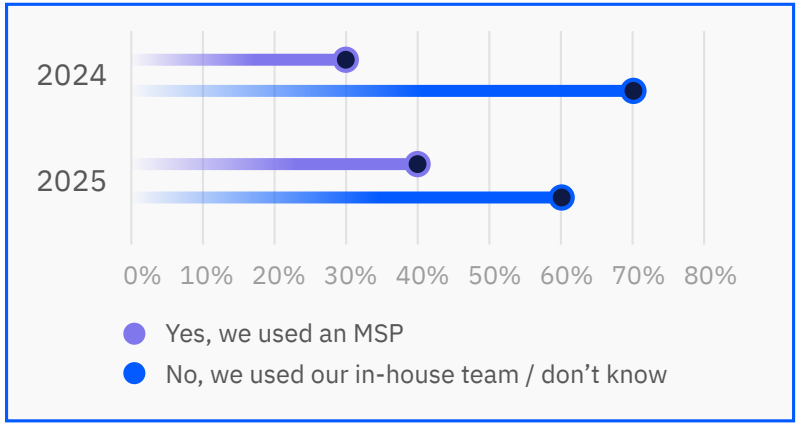
Agreeing on success metrics is a critical part of any cloud project, and the data paints a broadly positive picture. 88% of organisations have either recently completed a cloud infrastructure project, are currently undertaking one, or are planning one in the near future - up from 84% in 2023 and 2024.

Encouragingly, the rising number of cloud projects hasn't led to more failures. 87% of organisations report achieving all or almost all of their business objectives, an increase from 82% last year.

However, only 33% say they achieved all of their objectives - a reminder that there's still room to raise the bar. So how do organisations bridge this gap? And what strategies can help push projects from "mostly successful" to "fully realised"?

Enhancing Success Rates

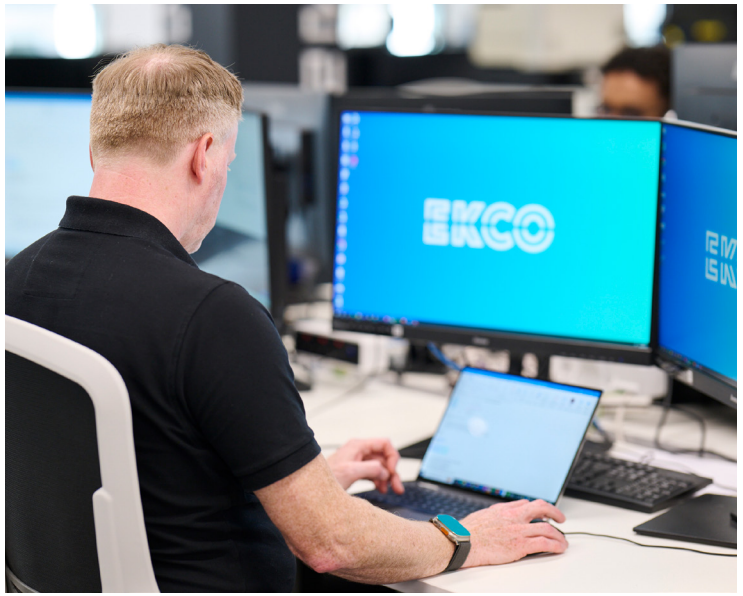
Did you use a Managed Service Provider (MSP) to help with your cloud project?



Closing that gap between 'most' and 'all' objectives being met, perhaps counterintuitively, starts well before the project is underway, rather than during a post-project analysis. Setting clear targets can eliminate unrealistic expectations and reduce the risk of projects going over budget.

MSPs are indispensable in this process. They can help provide clearer scopes for migration projects, set manageable goals and deadlines. Critically, MSPs take a significant burden from internal teams, who are often simultaneously facing day-to-day operational challenges and constraints, which leads to a higher likelihood of errors or missed details at the planning stage.

Over time, more and more companies seem to be recognising these benefits. In 2024, just under a third of organisations used MSPs to help with cloud projects. In 2025, that number has leapt up to 40%.



Internal vs. MSP-Managed Projects

The research found that projects are

6.6% more likely to achieve all their objectives with the support of MSP

8.3% more likely to be delivered within the original scope and initial timeline specified with the support of an MSP

> *"Cloud projects supported by MSPs are 6.6% more likely to achieve their objectives, thanks to clearer project scope and defined deliverables. MSPs provide clarity that in-house teams, often burdened by operational constraints, struggle to match."*
>
> **Peter Thomas,** *Senior Manager Cloud & Security Architecture at Ekco*

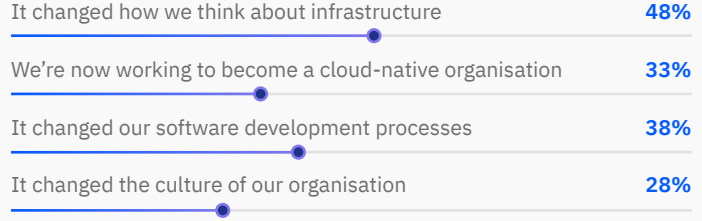
The data illustrates the advantages clearly. Companies that used MSPs to help with projects were 6.6% more likely to achieve their objectives than those just using internal teams. On top of this, they were 8.3% more likely to achieve these objectives without running beyond the specified timeline or over budget.

As the variety of options for cloud adoption grows, MSP partnerships are becoming more vital by the day in helping businesses navigate the landscape.

Wider Cultural and Operational Benefits

82%

of organisations, moving to the cloud helps them to create an agile culture.



The value of a successful cloud project can extend beyond its original objectives. Many organisations report broader, less tangible benefits such as increased agility, stronger collaboration, and cultural shifts in how teams engage with technology.

A third of respondents said their migration efforts sparked a move toward more cloud-native infrastructure, and nearly as many observed organisation-wide mindset changes. Nearly half reported a fundamental shift in how they think about infrastructure overall.

With the right MSP partner, businesses can maximise the return on investment while also unlocking additional value – from greater employee satisfaction to a more progressive, innovation-ready IT culture.

CHAPTER 3

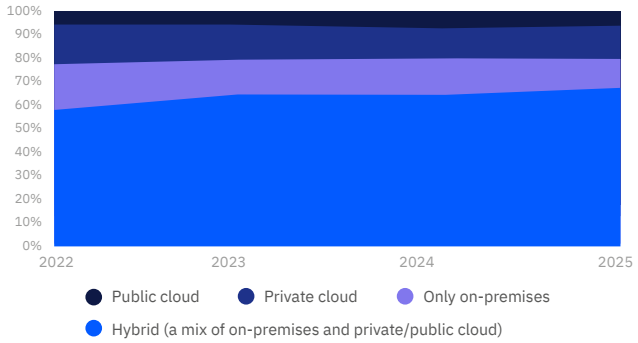
Optimising cloud

Optimising cloud infrastructure is critical to fully realising the benefits of cloud adoption. With increased cloud maturity, our 2025 survey indicates that 68% of organisations now adopt hybrid cloud environments, combining public or private clouds with on-premises solutions to balance cost, security, and performance effectively.

What strategies can organisations use to optimise their cloud environments and unlock greater efficiency? What common challenges slow down progress, and how can they be addressed effectively? And as businesses evolve their hybrid cloud setups, what practical steps can help ensure performance, cost, and security stay in balance?

Strategic Hybrid Cloud Adoption

Infrastructure Mix



Hybrid cloud has become a widely adopted model – and for good reason. It offers the scalability and flexibility of public cloud, combined with the control and security of private or on-premises infrastructure.

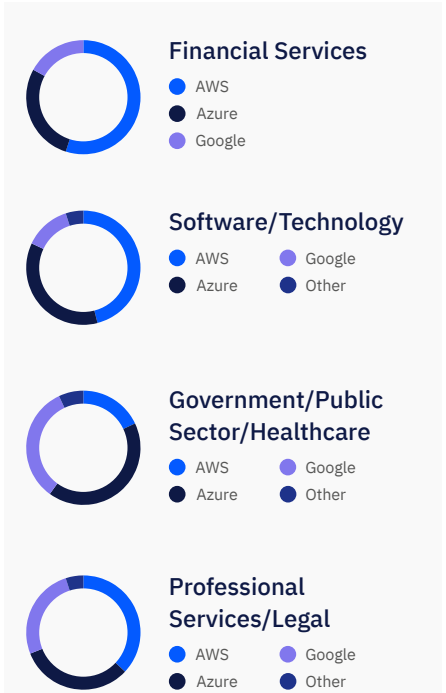
However, decisions around hybrid architecture should be driven by business requirements. There are many advantages to a hybrid cloud model, but they need to be evaluated within the context of a well-defined, fully costed strategy. An experienced MSP can help organisations assess the role each environment should play and ensure alignment with long-term goals.

Industry Preferences

How do you decide which cloud platform to use? Whilst many will perform well across an extremely wide variety of tasks and sectors, there is evidence to suggest that certain platforms are better suited to the needs of particular industries.

The preferences are most stark in Financial Services and Software Development. AWS is significantly more popular among financial service firms than other hyperscale providers, whereas Azure is favoured by software and technology companies.

Not all clouds are created equal for a given use case. Regardless of sector, optimising cloud solutions requires a detailed analysis of the platform's strengths and suitability to integrate with your existing architecture, rather than simply looking at factors like pricing or features.



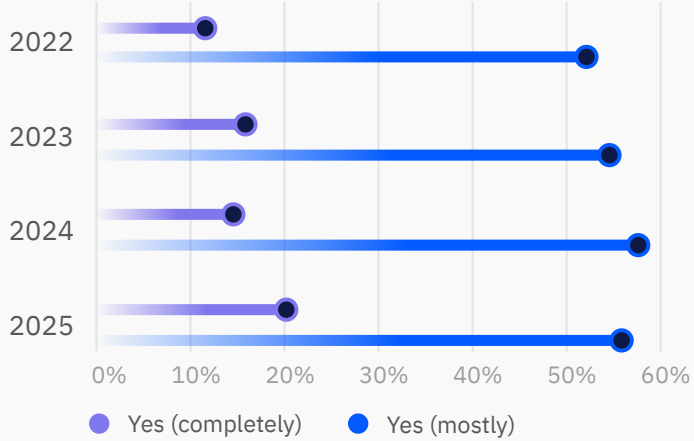
Challenges in Cloud Optimisation

Organisations are feeling their cloud setup is more optimised for success

76% feel it's optimised for success

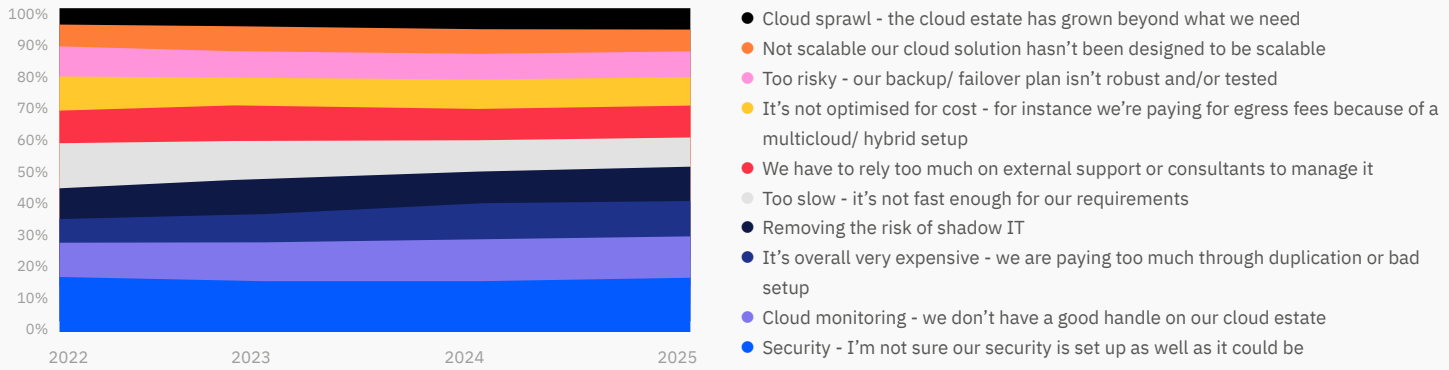
20% say it's completely optimised

Do you feel your current cloud set up is optimised for success?



When self-assessing the extent to which their cloud setup is fully optimised, we see similar results to those relating to a cloud project's success that we encountered in Chapter 2: over three quarters of firms believe that their cloud is optimised (up from 71% in 2024) – but a closer look reveals that of these only 20% think they're fully optimised. Once again, the key question is how more businesses can achieve that final step that takes a cloud project to the next level.

Where are you lacking optimisation?



Top Three Challenges In Cloud Optimisation

1. Security sidelined

Over a third of IT leaders say their cloud security setup needs improvement. As threats evolve rapidly, security too often becomes an afterthought – or is treated as a separate project altogether. The fix? Build it in from day one. Partnering with an MSP or MSSP ensures security is foundational, not bolted on.

2. Limited visibility

Lack of real-time insight into cloud performance is a growing concern. Hidden inefficiencies and blind spots in monitoring can lead to costly downtime. Modern cloud environments demand robust monitoring tools and processes to stay ahead of issues before they escalate.

3. Unclear costs

More than half of organisations say they lack visibility into cloud spend. Without clear, granular cost tracking, it's nearly impossible to measure ROI or optimise usage. Advanced cost-monitoring tools are key to staying in control – and on budget.

> *"Cloud infrastructure provides great opportunity for scaling and costs savings when implemented correctly, but when implemented incorrectly, costs can quickly spiral out of control and impact the bottom line. An MSP can provide continuous insights into your costs and provide recommendations to keep your estate efficient."*
>
> **Iain Evan,** *Azure Cloud Practice Lead at Ekco*

> *54% of IT decision-makers still lack complete visibility into their cloud spend, significantly hindering optimisation efforts. Enhanced monitoring and advanced analytics are vital to effectively managing cloud costs and improving ROI."*
>
> **Peter Thomas,** *Senior Manager Cloud & Security Architecture at Ekco*

Optimisation Is Ongoing – and Strategic

Cloud optimisation isn't a one-time task, it's a continuous process that demands active monitoring, clear cost controls, and security embedded at every level. As technology evolves, so do the opportunities to improve performance and efficiency of your infrastructure.

The right MSP doesn't just support this process – they simplify it. Acting as a strategic partner, they help teams stay focused on value, remove complexity, and ensure the cloud continues to deliver against business goals.

CHAPTER 4

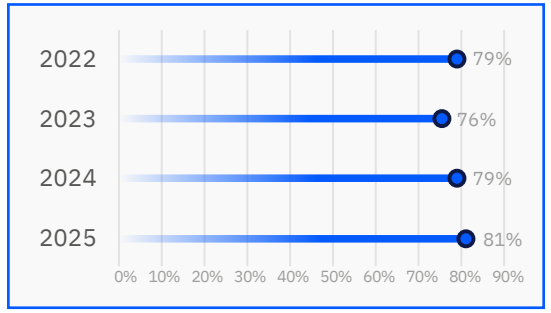
Cloud security

As organisations expand their reliance on cloud solutions, security threats and challenges have intensified. The research underscores the increasing complexity of cloud security, with 81% of IT leaders concerned about cyber resilience. Most notably, AI-driven threats now surpass traditional data breaches as the primary cloud security concern, reported by 59% of respondents.

> *"AI-driven cyber threats have overtaken traditional data breaches as the most critical cloud security concern. Businesses now face increasingly sophisticated, automated attacks that demand equally advanced defensive strategies."*
>
> **Keith Batterham,** *Lead Security Architect at Ekco*

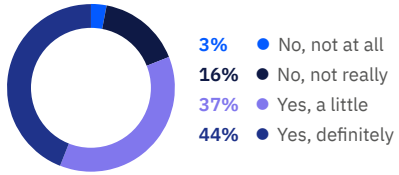
Increasing Cybersecurity Concerns

Concerns about cloud infrastructure security



In the last few years, businesses' concerns about the security of their cloud infrastructure have remained steadily high, with over three-quarters of leaders consistently expressing either slight or significant consternation about their infrastructure's resilience to cyber threats. In 2025, we saw a slight increase in this trend, and a record low 3% of respondents said they're 'not at all' concerned about their security.

Are you concerned about cyber security when it comes to your infrastructure?

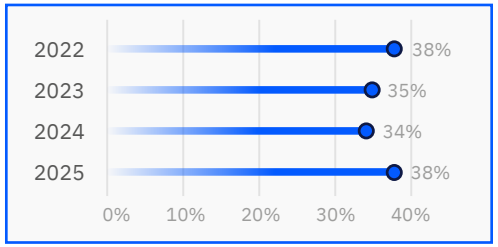


While this reflects the growing sophistication of cyber threats, it also points to a maturing mindset. Increased awareness is a positive development – it shows that organisations are taking security seriously and recognising it as a central pillar of their cloud strategy.

As threat actors adopt AI tools of their own, organisations need to keep their defences one step ahead. MSSPs play a crucial role here – not only by helping firms identify and address vulnerabilities, but by ensuring security is woven into the wider fabric of cloud operations. This joined-up approach doesn't just reduce risk – it drives smarter, more resilient ways of working across the business.

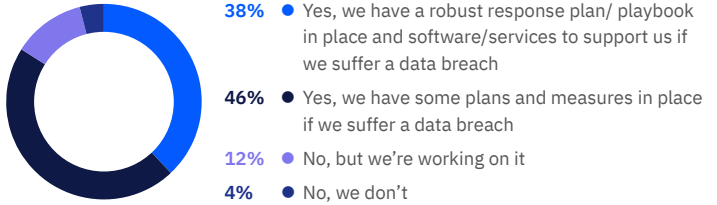
Cybersecurity Preparedness and Response

How prepared do firms feel in the event of a breach



> *"While 85% of organisations have cybersecurity breach plans, just 38% believe these plans are robust enough. Organisations need to evolve their cybersecurity strategies continuously to keep pace with the complexity of threats."*
>
> **Matt Saunders,** *Security SME at Ekco*

One data point that has held steady in recent years is how organisations feel about their ability to respond to a security breach. Just over a third of leaders say they have a robust plan in place, while the majority admit their preparations are partial at best – and in some cases, non-existent.



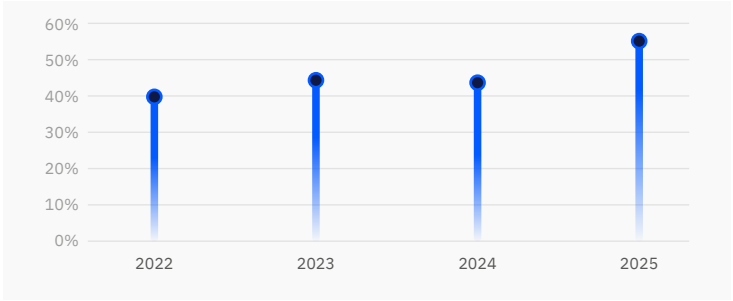
> *"Cybersecurity preparedness is concerning - 85% of organisations have breach response plans, yet only 38% trust their effectiveness. Organisations must regularly reassess and strengthen their cybersecurity frameworks to stay ahead of evolving threats."*
>
> **Peter Thomas,** *Senior Manager Cloud & Security Architecture at Ekco*

As cyber threats grow in complexity and frequency, having a clear, confident response plan is more important than ever. For those unsure about their readiness, the starting point is simple: regularly reassess systems, shore up the most vulnerable areas, and take guidance from current best practices.

Even among those with strong plans, ongoing refinement is essential. Threats evolve fast – and security plans need to evolve just as quickly. With the right support, organisations can turn uncertainty into resilience and ensure that if the worst happens, they're ready to respond swiftly and effectively.

Cybersecurity Insurance Trends

Do you have cyber security insurance in place?



In recent years, more organisations have turned to cybersecurity insurance as a key part of their risk management strategy. Adoption has grown steadily – rising from 43% to 55% in the past year – reflecting a growing awareness of the financial and reputational impact cyber incidents can have.

For IT decision-makers, this signals a welcome shift in mindset. More businesses are planning for the possibility of an attack – but the focus can't stop there. While insurance can help manage the fallout, it doesn't improve an organisation's security posture or reduce the likelihood of a breach occurring in the first place.

To build true resilience, organisations need to balance contingency planning with continued investment in proactive security measures. Because in cybersecurity, as in so many areas of business, prevention is always better than cure.

From Coverage to Confidence: Strengthening Your Security Posture

While cybersecurity insurance plays a valuable role in managing risk, it should sit alongside a broader effort to improve overall security posture. Insurers today also increasingly require organisations to demonstrate they're actively protecting their environments to qualify for coverage. For IT leaders, the next step is about putting practical measures in place that not only respond to threats but actively reduce the likelihood of them occurring.

Some of the most effective strategies are also the most accessible. Alongside maintaining insurance and securing third-party access, workplace culture remains a crucial factor. Building awareness and embedding strong security habits across the organisation can make a meaningful difference.

Here are four core practices that help reinforce a stronger, more resilient security posture:

Assumed Breach Mindset:

No system is entirely immune to attack. Operating under the assumption that a breach will occur – and running regular incident response exercises – helps teams stay alert, improve mitigation, and reduce potential impact.

Zero Trust Architecture:

This approach requires all devices, users, and systems to be verified before access is granted. It limits lateral movement within networks and significantly lowers the risk of unauthorised access.

Multi-Factor Authentication (MFA):

MFA is now a baseline requirement for organisations – but it needs to be universally and consistently applied. Ensuring it's enabled across all platforms helps close a common entry point for attackers.

Attack Surface Management (ASM):

You can't defend what you don't know exists. ASM is the practice of identifying, and continuously monitoring all potential entry points especially in complex environments, especially those with cloud assets, remote endpoints, and third- party tools, then securing them.

CHAPTER 5

Cloud & AI: New frontiers

Artificial Intelligence is fast becoming a core element of cloud infrastructure strategies. Once limited to specific use cases, AI is now being embedded more broadly across enterprise environments – driving efficiency, enabling smarter operations, and opening new opportunities for innovation.

As adoption grows, so do the challenges. Many organisations are now working with multiple AI platforms, reflecting a shift toward a more flexible, multiplatform approach. At the same time, concerns around data accuracy, security, and the complexity of model adoption remain high on the agenda.

To get real value from AI in the cloud, organisations need to be deliberate - matching fast-moving innovation with the governance and trust that enterprise environments demand.

Accelerated Adoption of AI

AI is growing in use in organisations

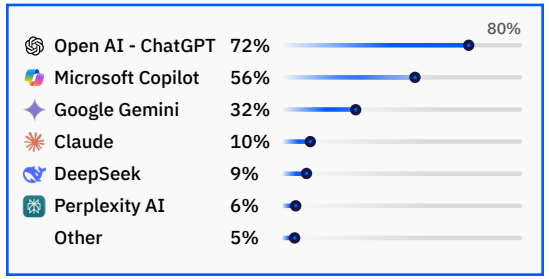
58% of IT decision makers now actively using AI for work

46% up from year ago

AI has rapidly moved from exploration to execution for a growing number of organisations. Improved accuracy, faster deployment, and a widening range of practical use cases have helped push adoption forward – with more than half of IT decision-makers now actively using AI in their workflows.

The AI marketplace itself has matured at remarkable speed. ChatGPT leads in adoption, used by over 70% of firms, followed by Microsoft Copilot (55%) and Google Gemini (just over 30%). Each platform is carving out its own niche, with adoption often varying by sector and workload.

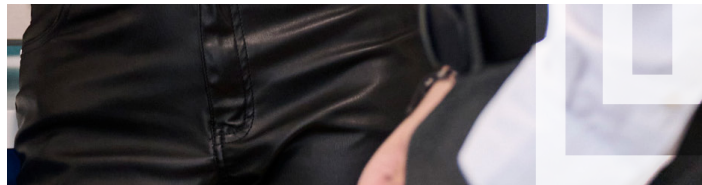
Top AI Platforms



At the same time, the market itself is changing. New challengers like DeepSeek – which has already become the fifth most-used AI platform despite launching just this year – highlight the growing appetite for open-source and specialised models. These alternatives are helping businesses tailor AI to their specific needs, accelerating adoption even further.

Perhaps most notably, the way organisations are using AI is evolving. Rather than relying on a single platform, many are taking a more flexible, use-case-driven approach – combining tools to match specific tasks and extract maximum value across the enterprise.

> *"Businesses are increasingly adopting multiple AI platforms - up from 16% to 28% - indicating a shift towards flexibility and away from reliance on single-vendor ecosystems. This multi-platform approach aligns better with specialised workloads."*
>
> **Keith Batterham,** *Security Practice Lead at Ekco*



Unlocking Real Value: The Business Case for AI Integration

81% highlighting enhanced productivity

77% saw improvements in everyday efficiency

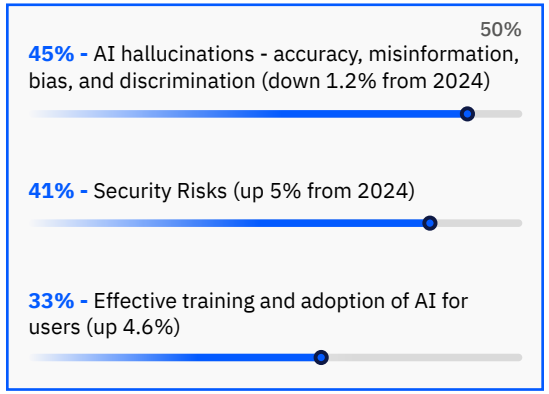
The surge in AI adoption isn't simply driven by curiosity – it's grounded in clear, measurable benefits. Among organisations already using AI, 81% report enhanced team productivity, while 77% have seen improvements in everyday efficiency.

By automating routine or repetitive tasks, AI allows teams to focus on higher-value, more complex work – freeing up time, boosting output, and enabling faster decision-making across the business.

> *"Organisations are shifting towards agentic AI workloads, automating complex workflows to decrease reliance on human oversight. The next wave of AI will see increased autonomy, demanding higher trust in AI systems."*
>
> **Keith Batterham,** *Lead Security Architect at Ekco*

As adoption matures, many businesses are already looking beyond basic automation. The rise of agentic AI – capable of executing end-to-end tasks with minimal input – signals a shift toward deeper integration and more autonomous systems. For IT leaders, this underscores the need to build AI strategies that balance innovation with governance, and speed with trust.

Navigating the Risks: AI's Growing Pains



As enthusiasm for AI continues to grow, IT leaders remain clear-eyed about the risks and challenges of using the technology. Concerns about accuracy – particularly AI hallucinations, misinformation, and bias – top the list, flagged by 45% of respondents. The good news: this figure is slightly down from last year, reflecting early gains from more advanced models and improved safeguards.

Organisations have turned to AI to boost productivity, hackers are doing the same to bypass security defences. Techniques like deepfake audios and executive impersonation are used to trick staff to share sensitive information. This threat is reflected in the data, where concerns are also on the rise, up 5% from 2024. This is likely driven by the increased integration of AI into sensitive workflows and data environments At the same time, more organisations are recognising the human factor: a third of firms now highlight effective training and adoption as a key challenge – up nearly 5% year-on-year.

The message is clear: to scale AI safely and successfully, organisations must invest not only in the technology itself, but in the people, processes, and governance needed to manage it responsibly.

> *"AI hallucinations remain a significant concern for 45% of IT leaders. However, improved validation techniques such as retrieval-augmented generation (RAG) and human oversight are reducing inaccuracies and biases."*
>
> **Keith Batterham,** *Lead Security Architect at Ekco*

Best Practices for Safe AI Integration

As with any rapidly evolving technology, AI brings both opportunities and unknowns. The full scope of risks may not yet be understood, which makes ongoing vigilance essential. Businesses need to monitor the shifting landscape, assess how AI is used across teams, and stay responsive to emerging challenges.

One of the most effective safeguards is education. A workforce that understands how to use AI responsibly – from avoiding sensitive data inputs to recognising when to apply human oversight – is better equipped to adopt good practices and respond quickly when things go wrong.

Still, training the workforce remains a challenge. A third of IT leaders cite difficulty in implementing effective AI training across their organisations. The key is to make learning part of the workflow – integrating AI tools in a way that complements existing systems and supports, rather than disrupts, day-to-day work.

Agile and Data-Driven Culture

To deliver lasting value, AI adoption must be grounded in clearly defined business objectives. Data should guide every step – from platform selection to deployment strategy. This helps organisations avoid the trap of chasing hype and ensures each tool is solving a real, measurable problem.

A multiplatform approach can also reduce risk. By spreading workloads across different AI tools, organisations avoid overreliance on any single provider and gain flexibility to tailor solutions to specific needs – whether it's automating internal tasks, enhancing customer service, or improving analytics.

AI implementation can be complex but with the right internal focus, a commitment to continuous learning, and a clear view of business outcomes, IT leaders can embed AI in a way that drives long-term value without compromising control.

Conclusion

Cloud infrastructure is now one of the foundations of modern businesses - but it's a foundation still under construction. For most organisations, the days of "lift and shift" are behind them. What lies ahead is a more winding road, shaped by the rise of hybrid cloud, the growing role of AI, and persistent challenges around visibility, skills and security.

This year's findings show that while the groundwork has been laid, many organisations are now focused on reinforcing and refining their infrastructure - making it more resilient, more efficient, and more responsive to the evolving demands of the business.

Momentum is strong. As we saw, 88% of organisations have recently completed or are currently engaged in cloud infrastructure projects, and 87% report achieving all or most of their objectives. But only a third hit every goal, and just 20% feel their infrastructure is fully optimised. These figures reflect a cloud estate that's operational but not yet fully matured.

Hybrid cloud adoption continues to rise - now at 68% - as organisations seek to balance flexibility, control and cost. At the same time, 58% are actively using AI, often across multiple platforms, introducing new considerations around integration, governance and risk.

Yet the benefits of this transformation remain unevenly distributed. Over half of IT decision-makers (54%) lack full visibility into their cloud spend, while only 27% feel they have the internal skills to scale cloud effectively. Without better visibility and capability, organisations risk introducing inefficiencies that undermine long-term value.

Security, too, is under pressure. 81% of IT leaders are concerned about cyber resilience, with AI-powered attacks now seen as the most significant threat. While 85% have a breach response plan, just 38% believe it's robust. It's clear that defences need to evolve in step with the infrastructure itself, and security must be embedded, not added on.

That's why more organisations are leaning on external partners. 40% now work with Managed Service Providers (MSPs) - up from 30% last year. The benefit is clear: cloud projects supported by MSPs are more likely to stay on track, on budget and deliver against their full set of objectives. These partnerships don't just extend technical capability, they help organisations see further, act faster, and avoid costly missteps.

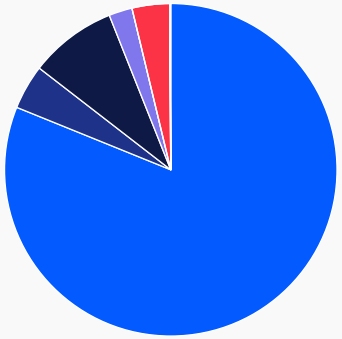
Modern infrastructure is no longer just about getting to the cloud, it's about what you build once you're there. It's a strategic asset, but only if it's continually shaped, maintained and optimised to support your goals. That means staying proactive, working with the right partners, and building in adaptability from the ground up.

For IT leaders, the challenge today is not just to keep pace, but to build with purpose. By approaching modernisation as a continuous, iterative process, organisations can turn complexity into clear progress, manage risk with greater resilience, and use infrastructure as a practical driver of innovation and growth.

Appendix

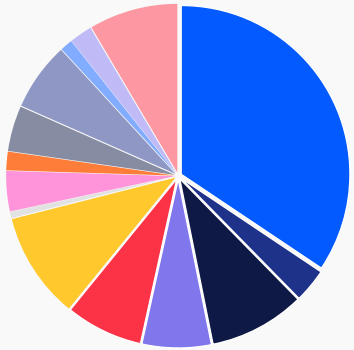
Survey Demographics

Where do you live?



81.13% England
4.35% Wales
8.50% Scotland
2.27% Northern Ireland
3.66% Ireland
0.10% Other

What industry do you work in?



34.39% Software/Technology
3.26% Consulting
9.19% Education/University
6.62% Financial Services/ Insurance
7.41% Government/Public Sector
10.18% Healthcare
0.59% Legal Services
3.85% Media, Arts or Marketing
1.78% Non-profit
4.35% Professional Services
6.52% Retail
1.19% Scientific
2.17% Transportation
8.50% Other

What size of organisation do you work for?

18.18% 1-49
10.57% 50-99
20.45% 100-499
12.45% 500-999
15.91% 1,000-4,999
22.43% >5,000

EKCO

info@ek.co
www.ek.co
+44 (0)330 135 8792
106 Saxon Gate, Milton Keynes