READINESS REPORT

Unlocking Cloud Readiness

kyndryl

2025

Contents

Introduction

Key takeaways

Cloud success is strongest when not accidental. A deliberate strategy aligns infrastructure, data, and governance — driving innovation, enabling AI, and anchoring a secure, compliant IT estate.

Agentic AI depends on deliberate design. When architecture connects systems and data seamlessly, intelligence can move — and innovation can scale.

Security and sovereignty are design principles, not constraints. Cloud strategies should be designed for trust and interoperability from the start, allowing organizations to balance compliance, resilience, and performance while advancing innovation.

Agility, innovation, and cost control.

These are the goals of all enterprises. And for driving business success, cloud computing has been remarkably effective at delivering on all three. There's a reason cloud services have grown into a more than $700 billion industry today. In fact, companies have increased their cloud spend by more than 30% in the past year, according to the Kyndryl Readiness Report. An overwhelming majority of enterprises globally use the cloud to store, manage, and effectively process their data, and deploy innovative solutions.

Partnering with cloud providers, particularly hyperscalers, provides enterprises with access to cutting-edge solutions and services without the capital investments they would otherwise require. Across public, private, and hybrid models, cloud solutions now meet most enterprise needs — enabling continuous innovation in a competitive global market.

In fact, enterprises that treat cloud as a strategic backbone — aligning business and IT, modernizing pragmatically, embedding AI, and co-innovating with their ecosystem — achieve markedly greater innovation, agility, and value than those that use cloud in a more reactive or fragmented way. And yet, 70% of CEOs admit they arrived at their current cloud environment "by accident, rather than by design."

But if companies benefitted from happenstance in the past, those days are over. Cloud success is no longer a matter of luck but design. The enterprises that thrive now are those that approach cloud as the foundation for intelligence, adaptability, and trust.

Maximizing return from cloud investment requires a shift in mindset. The most effective strategies unify business and IT, treating cloud not as infrastructure but as a vehicle for transformation. This evolution expands how organizations create value — demanding deliberate platform adoption that delivers innovation with control. Integrating cloud strategy with business priorities helps businesses adapt faster and capture more value from their investments.

But it's a complex challenge. The road to an optimal cloud strategy is often uneven, shaped by past decisions, legacy systems, and the practical limits of cost and control. Enterprises relying on large cloud providers can feel locked into vendors, as proprietary tools can make switching services expensive and unwieldy.

The advent of AI has given enterprises more to consider as it challenges previous assumptions about data management; and geopolitical developments place new regulatory demands on where and how data moves. Enterprises are demanding new flexibility and interoperability. Increasingly, they want a seamless user experience, where the differences in platform are invisible and imperceptible.

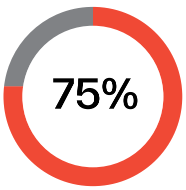
This convergence of inflection points is creating a new world of competing priorities. For many enterprises, their current cloud configuration wasn't the result of a grand design — it just happened over time. But now is not a time to retrace steps; it's about choosing direction. Leaders across industries are eager to leverage this moment into an intentional advantage.

One thing is clear: cloud utilization is on the rise. But for enterprises with rapidly changing requirements, what the cloud looks like and who provides it may be very different in the years to come.

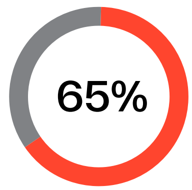
Architecture defines control

These are dizzying times for executives. Technological innovation barrels toward them faster than they can absorb it. Blockchain, the metaverse, generative AI, agentic AI, quantum computing; each development comes with its own demands and challenges. At the same time, geopolitical disruptions are destabilizing the foundations upon which many enterprises are built.

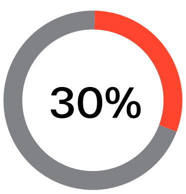
In this environment, there is a growing unease among some cloud users about their current strategy. Their disquiet is amplified by new digital and technology sovereignty measures that may tie data — and the people who can access it — to specific geographies. Consequently, leaders are experiencing a shift in thinking.



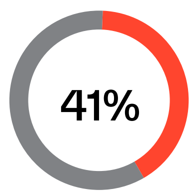
Leaders who report feeling concerned about the geopolitical risks associated with storing and managing data in global cloud environments



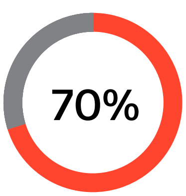
Leaders who report they've made changes to their cloud strategies due to new geopolitical pressures, including data sovereignty regulations



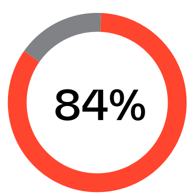
The amount on average that organizations increased their cloud spend over the last year



Leaders who report they are repatriating at least some of their data from the cloud to on-premises servers



CEOs who say they believe they arrived at their current cloud environment by accident, rather than design



Cloud leaders who say they intentionally choose to use multiple clouds

Source: 2025 Kyndryl Readiness Report; Kyndryl Cloud Innovation Survey

Architecture defines control

The modern enterprise wins not by choosing where to build, but by knowing how. Innovation moves fast, but architecture decides who stays in control.

What once seemed like a tension between the reach of cloud computing and the control of on-prem systems has matured into a focus on architectural intent. It is not about on-prem OR the cloud, it is about on-prem AND the cloud. The most forward-thinking organizations are realizing that the winning strategy is about access to the right capabilities, irrespective of where they are, and retaining control and security over their architecture. To that end, strategic platform choices are key. The right cloud partner can be a catalyst for innovation, helping reduce the cost of complexity while accelerating new capabilities. Understanding the capabilities of potential partners, and weighing their relative advantages, is a critical step for an enterprise mapping its future.

The new value lies in intelligent design through complexity management, which encompasses FinOps, agentic AI operations, and platform consistency. Innovation today isn't defined by where IT workloads live, but by how they're managed and optimized across diverse environments. Across industries, that evolution is taking shape in tangible ways — from how global hyperscalers localize infrastructure to how enterprises integrate private and public environments:

- **Hybrid integration unlocks performance and compliance.** Private clouds can now be seamlessly integrated with public platforms, enabling enterprises to use the best environment for each workload. Even in countries with stringent data rules, not all information must be isolated. The optimal approach is an intentional mix of platforms designed to maximize performance and minimize risk.

- **Enterprises can now link private data to public AI securely.** Technologies are being developed to bridge data on private clouds with the AI products that run on public clouds. Enterprises can therefore access the advantages of large language models (LLMs), which are powered by vast reams of public data, without risking their own data becoming compromised.

- **Global hyperscalers are providing higher levels of local sovereignty.** These companies have invested billions in infrastructure to build cloud servers to allow their customers to store data locally. Providers are also building industry-specific clouds to cater to the needs of their customers.

AI and the cloud

No matter the mode — public, private, or hybrid — the cloud has become the foundation for AI. The difference lies in how enterprise leaders design for it. Strategic decisions about where workloads live, how they interconnect, and how data is governed determine whether AI can scale responsibly, with the right governance, and at pace.

For some enterprises, however, there are obstacles to accessing the LLMs that live on the cloud. Every organization must prioritize some degree of control, and some face government restrictions on where data can be located. For those, there are now language models that can live on private clouds, allowing enterprises to craft their own AI capabilities. These provide enough capability to be transformative — particularly when paired with methods such as retrieval-augmented generation (RAG), which allows models to access and update information dynamically without retraining.

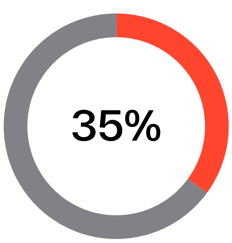
Others, driven by the need for greater computational power to train or run AI models, are turning to neoclouds. These focus specifically on GPUs and are optimized for AI workloads. Through neoclouds, organizations can rent GPU power on-demand without investing in infrastructure or locking into long term cloud contracts, making it easier for startups and research labs to scale quickly.

In every case, the common denominator is strategy. Cloud architecture is the foundation that determines how intelligently, securely, and sustainably AI operates across the enterprise.

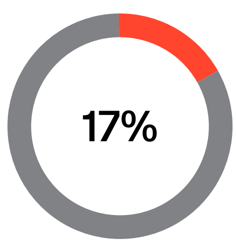
The rise of agentic AI

Agentic AI creates its own opportunities and challenges. As it becomes increasingly common, harnessing AI to build agents will become a critical tool for cutting costs, maximizing efficiency, and driving innovation. But agents assigned to specific and narrow tasks may not need to access all the data in an LLM, which can be costly and inefficient. Rather, it may make more sense for them to operate in a private cloud environment, where the benefits of speed and data control outweigh the advantages of a larger public cloud.

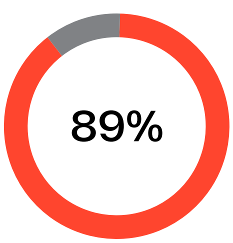
That's why the evolution of agentic AI isn't just about smarter models — it's about smarter infrastructure.



Leaders who cite integration challenges as a stop barrier to positive ROI on AI



Leaders who report having a cloud-first approach to their IT infrastructure



Leaders who say cloud investments have allowed them to use AI more easily

Source: 2025 Kyndryl Readiness Report

AI and the cloud

The future of AI won't be defined by algorithms alone, but by the environments that host them. AI runs on data — but it thrives on design.

To balance performance, security, and cost, many leaders will need a hybrid cloud foundation that bridges public and private environments seamlessly.

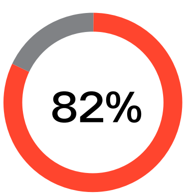
Agentic systems often learn and reason well in the public cloud, where near-limitless compute and synthetic data environments make it possible to safely train models at scale. But once trained, agentic AI needs to operate close to an organization's own data. In the context of private clouds, that includes protecting sensitive information, enforcing compliance, and maintaining control over decision-making processes. In effect, training in the public cloud builds intelligence, while inference in the private cloud keeps that intelligence grounded in secure, real-world context.

By linking the scale of public AI with the security of private infrastructure, enterprises can create a continuous loop between learning and doing. With people kept in the loop to guide, review, and correct the system — bringing empathy and judgment — this approach balances performance and control while building trusted, adaptive AI that can act autonomously without exposing the business to unnecessary risk.

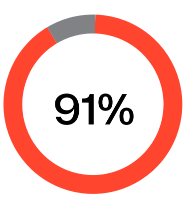
Redefining cloud security

Cybersecurity has been a Board-level priority for more than a decade, and with the advent of AI-fueled attacks it will only become a larger source of attention. Yet the same technologies that can expand the surface area of risk can also strengthen resilience. Cloud architectures provide enterprises more ways to isolate threats, restore systems, and maintain continuity even under attack. Resilience today depends on flexibility and control — the ability to adapt quickly to new risks while maintaining governance over how data, systems, and AI models behave.

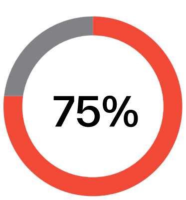
The next generation of cloud will be defined less by where workloads run and more by the experiences they deliver. True hybrid cloud means providing the same seamless, secure experience — and the same operational continuity — whether data and applications reside on a public, private, or multi-cloud environment.



Leaders who report they have managed a cyber-related outage this year



Leaders who report their cloud infrastructure provides flexibility to adapt quickly to new or changing regulatory requirements



Organizations that report they are investing in AI for cybersecurity — more so than any other AI capability

Source: 2025 Kyndryl Readiness Report

It's not just about security and resiliency in the traditional sense, but about enabling consistent performance, interoperability, and trusted data flow between providers. This ability to move and manage data freely across suppliers will become a hallmark of next-generation cloud architecture — a shift that new regulations, including the EU Data Act, are poised to accelerate.

Cloud users have a variety of overlapping security concerns:

- **Scale cuts both ways.** Cloud providers are under constant attack from hostile actors looking to exploit vulnerabilities. Hyperscalers have invested huge sums to mitigate the risk, but their very size makes them an attractive target.
- **AI doesn't always know where the lines are.** The nature of AI means private data can be accidentally ingested by the models. That can happen when users are plugging proprietary data into publicly available web-based AI tools or through interfaces like APIs. That's why modern AI strategies must start with governance — treating data custodianship as a core security function, not an afterthought.
- **The cloud is global, but the laws that govern it aren't.** Shifting geopolitical currents means assumptions about the privacy and integrity of privately stored data may no longer be valid. The threat of a government shutdown of cloud services, or government seizure into commercial data can no longer be dismissed out of hand.

Addressing the security needs of individual enterprises requires tailored solutions that meet their specific requirements.

Conclusion

The age of hybrid isn't a transition — it's the foundation for an agile and adaptive enterprise.

Leaders are no longer asking whether to move workloads between public and private environments, but how to make those environments operate as one. AI, data sovereignty, and security are converging to redefine what cloud means — from a place where data lives to a living architecture that learns, adapts, and protects.

In every case, the differentiator is strategy: the deliberate design of cloud architecture that unites scale, security, and intelligence. As AI becomes more agentic, the cloud will not just host intelligence — it will help shape it.

The organizations that thrive in this new era will treat the cloud not as a static utility, but as a strategic capability — one built for interoperability, trust, and continuous reinvention. With the right architecture, hybrid cloud becomes the intelligent foundation of the AI-ready enterprise.

This report was not printed.

Company Headquarters

One Vanderbilt Avenue, 15th Floor
New York, New York 10017

kyndryl.com