PwC's 2025 Africa Cloud Business Survey

The new age of cloud: Responding to a shifting paradigm

Part 1 – Foundation adoption is strong: new complexity is slowing progress

Content

Executive Summary

1 **Introduction:** Cloud at a crossroads

2 **Cloud maturity:** From adoption to optimisation

3 **Geopolitics and regulation:** The new cloud borders

4 **Conclusion:** Strategic choices must balance AI adoption with sovereignty and economic considerations

Methodology

Glossary

Contacts

Cloud adoption across Africa continues to accelerate, however organisations face a unique set of challenges that demand careful navigation. Many are working within tight budgets whilst addressing a shortage of specialised cloud and security skills, managing rising cyber risks, and adapting to a shifting regulatory landscape.

What's emerging from this, however, is a maturation that goes well beyond basic adoption. Africa is now moving into an era of cloud mastery–where organisations aren't just implementing cloud solutions, but strategically leveraging them to address their most pressing business challenges.

Our cloud survey reports explore precisely how organisations across the continent are turning these multifaceted pressures into opportunities. We examine their approaches to sovereignty requirements, AI readiness, and financial discipline, revealing how forward-thinking leaders are converting constraints into catalysts for meaningful progress on their transformation journeys.

Mark Allderman
Africa Cloud and Digital Leader,
PwC South Africa

Executive summary

The new age of cloud: Responding to a shifting paradigm

Across the continent, cloud has moved beyond being merely infrastructure to become a central consideration in strategic transformation, driving value creation through digitalisation, insights, automation, and resilience. This represents a decisive shift from cloud adoption to optimisation.

However, the landscape is evolving rapidly. Geopolitical tensions and financial pressures are reshaping how organisations approach their cloud strategies, making it essential to balance the potential of advanced technology with robust governance frameworks.

Our survey highlights several critical trends emerging from this shift: the growth of multi-cloud environments, cloud's pivotal role in enabling AI adoption at scale, sovereignty considerations increasingly influencing architecture decisions, and governance alongside FinOps capabilities becoming essential rather than optional for sustainable cloud success.

Four key dynamics define the new age of cloud

Cloud strategies evolve with purpose

89%

of organisations are refining their cloud approach in response to geopolitical and regulatory change. Cloud has become a strategic lever for resilience, compliance, and competitiveness–not just a technology choice.

Infrastructure transformation accelerates

98%

of organisations plan to adjust and expand their cloud architecture and coverage, driven by scale, flexibility, and sovereignty. Many are adding multi-cloud capabilities or integrating sovereign solutions for specific use cases to meet diverse operational and regulatory needs.

Multi-cloud becomes the operating norm

86%

of organisations already run workloads across multiple cloud providers to enhance resilience, gain flexibility, and access best-in-class capabilities. Managing this complexity will increasingly determine cloud maturity and value realisation.

Agentic AI emerges as the next frontier

91%

of organisations say agentic AI capabilities are decisive for provider selection—yet only 37% are scaling it. Cloud is the foundational layer that turns AI experimentation into enterprise-wide intelligence.

Executive summary

Organisations across Africa are rapidly advancing in cloud maturity while navigating increasing complexity as they balance innovation with data sovereignty, security, and disciplined cost control. This evolution marks a decisive shift from basic migration to optimisation and trust-building—establishing foundations for agentic AI adoption and next-generation intelligent workloads.

Key Findings

Accelerating maturity:

79% of organisations reported medium or high cloud maturity in 2025, up from 50% in 2023, bringing Africa in line with EMEA benchmarks.

AI prioritisation:

AI adoption tops cloud priorities, with over one-third moving beyond early agentic AI pilots to enhance decision-making.

Geopolitical influence:

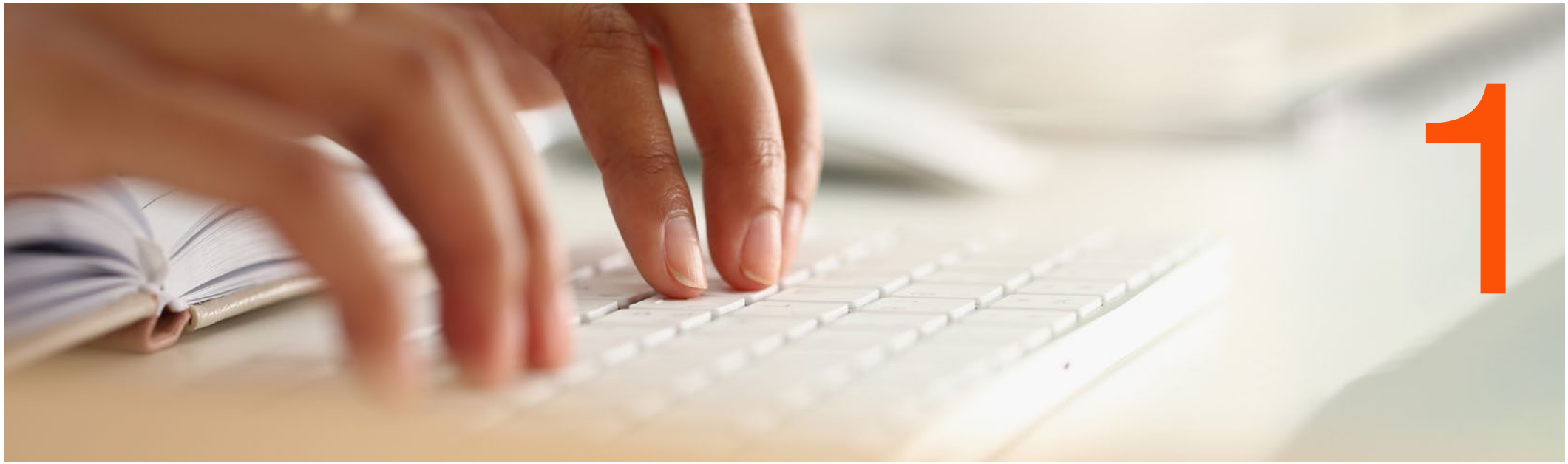
89% are refining cloud strategies in response to geopolitics and regulation, driving interest in sovereign and national solutions.

Investment surge with governance gaps:

86% plan increased cloud spending over the next 12 months, yet only one in ten have implemented advanced FinOps practices.

Risk-driven sovereignty:

Risk mitigation leads adoption of Sovereign Public Cloud or National Partner models, with performance optimisation guiding workload decisions.



1

Introduction: Cloud at a crossroads

Cloud maturity across Africa has accelerated dramatically. Most organisations have moved beyond basic adoption to strategic optimisation, closing the gap with global benchmarks in just two years.

But maturity brings new challenges. Geopolitical tensions and regulatory changes are forcing organisations to reconsider fundamental cloud decisions—where data is stored, which providers to use, and how to structure architectures for resilience.

The response has been clear: organisations are diversifying their cloud strategies. Multi-cloud deployments are becoming standard practice, not just for technical reasons but as hedges against political and regulatory uncertainty.

This shift marks a turning point. Cloud is no longer just about technology efficiency—it's about strategic resilience. Organisations must now balance performance and cost with compliance and risk management.

The organisations that master this balance will be better positioned for an uncertain future. Those that don't risk being caught unprepared when external pressures intensify.

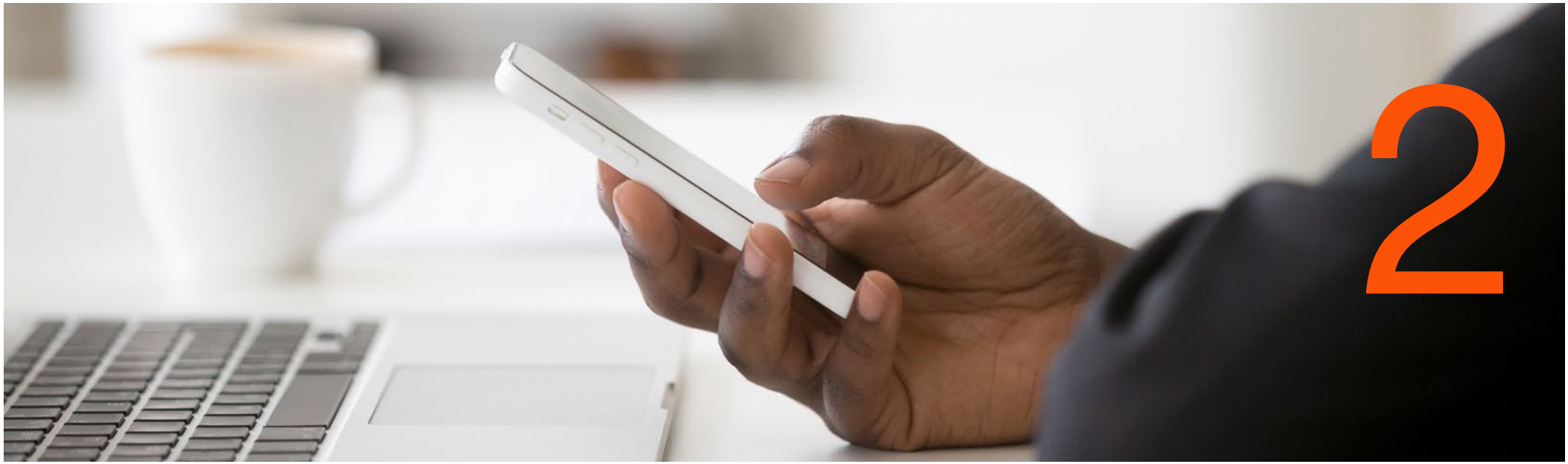
About the survey

The 2025 EMEA Cloud Business Survey of 1,415 business and technology leaders conducted in the July through September 2025 period.

Almost half of the leaders (44%) are from companies with $1 billion or more in revenue. Respondents operate in a range of industries, including industrial manufacturing and automotive (22%); financial services (21%); tech, media and telecom (18%); consumer markets (17%); energy, utilities and resources (10%); healthcare (8%); and government and public services (5%).

Respondents are based in 26 countries. The regional breakdown is Western Europe (54%), the Middle East (20%), Central and Eastern Europe (15%), and Africa (11%).

PwC Research, PwC's global Centre of Excellence for market research and insight, conducted this survey.



Cloud maturity: From adoption to optimisation

Maturity is rising fast; business leaders report higher maturity levels than technology leaders

80%

of organisations in Africa reported medium or high cloud maturity in 2025.

33%

report cloud being deployed across the enterprise.

Africa's cloud maturity is accelerating at unprecedented pace

Cloud adoption across Africa has transformed dramatically over the past two years, with organisations rapidly closing the gap with their EMEA counterparts and moving beyond basic implementation to strategic optimisation.

Dramatic maturity gains across the continent

- Over 80% of organisations in Africa reported medium or high cloud maturity in 2025–a significant jump from 61% in 2023.
- High maturity has nearly doubled from 14% to 27%, now matching EMEA levels.
- Larger organisations consistently lead in maturity, demonstrating the impact of sustained digital transformation investments.

A tale of two perspectives

Business and technology leaders often have conflicting assessments of their organisation's progress when it comes to tech migrations and digital transformation initiatives:

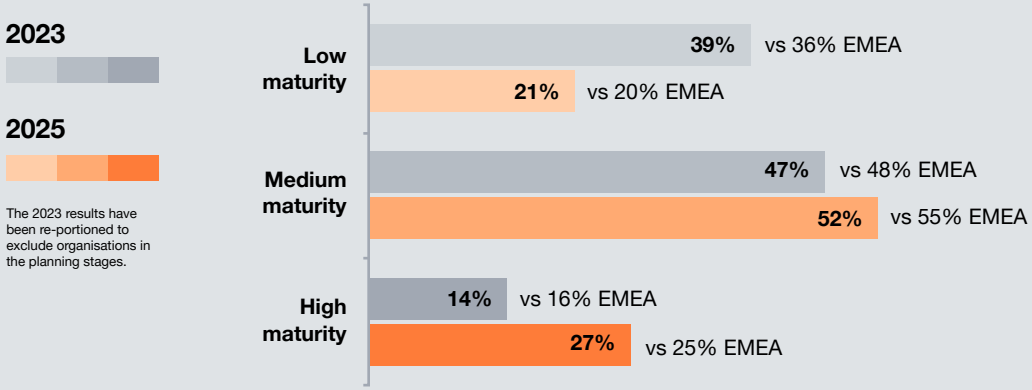
- Business leaders believe they're driving enterprise-wide success: 33% report cloud deployed across the enterprise, compared to just 21% among technology teams.
- Technology teams believe they're still building critical foundations: 58% operate at medium maturity (above Africa's 52% and EMEA's 55%), focusing on standardising platforms and modernising applications.
- This perception gap reveals that business leaders see themselves as more advanced at converting investments into organisation-wide outcomes, whilst tech teams view the organisation as still concentrating on creating scalable infrastructure foundations.

From adoption to strategic transformation

The region has moved beyond basic cloud implementation towards disciplined optimisation, using cloud to reshape business models and foster ecosystem collaboration. This rapid progression demonstrates that with aligned governance, talent development, and value management, organisations in Africa can transform strong adoption into consistent, enterprise-wide high maturity–unlocking cloud's full strategic potential.

Figure 1a.

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

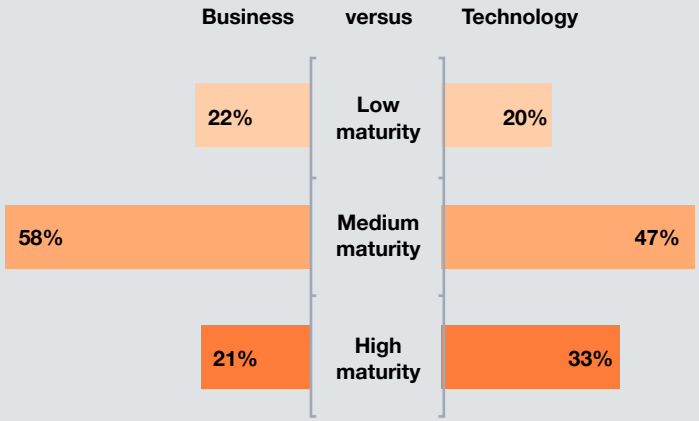


Base: All Africa respondents (2023 – 155,2025 – 162)

Source: PwC's EMEA Cloud Business Survey, September 2025

Figure 1b.

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



Base: All Africa respondents (Business – 89, Technology – 73)

Source: PwC's EMEA Cloud Business Survey, September 2025

Implementation of key cloud-related initiatives varies

Advanced capabilities reveal maturity gaps

While organisations in Africa demonstrate strong foundational cloud adoption, enterprise-wide implementation of advanced capabilities remains inconsistent. When examining AI enablement, FinOps, and carbon footprint measurement, adoption levels drop significantly across both business and technology leaders.

Implementation challenges in critical areas

- **AI and ML tools:** Only 37% of organisations have implemented these capabilities across many parts of their organisation.
- **FinOps practices:** Just 33% have established financial operations discipline enterprise-wide.
- **Carbon footprint management:** Measuring and reducing cloud-related emissions shows the lowest enterprise-wide adoption.
- **Strong foundations exist:** Over 85% of organisations have implemented these initiatives to some extent, indicating readiness for broader deployment.

Security investment prioritised but requires expansion

- Over 60% have strengthened cybersecurity, disaster recovery, and risk mitigation protocols.
- Investment concentrates on identity and access controls, threat detection and response, and resilience planning.
- Enterprise-wide security by design remains imperative to counter sophisticated and increasingly complex emerging cyber threats.

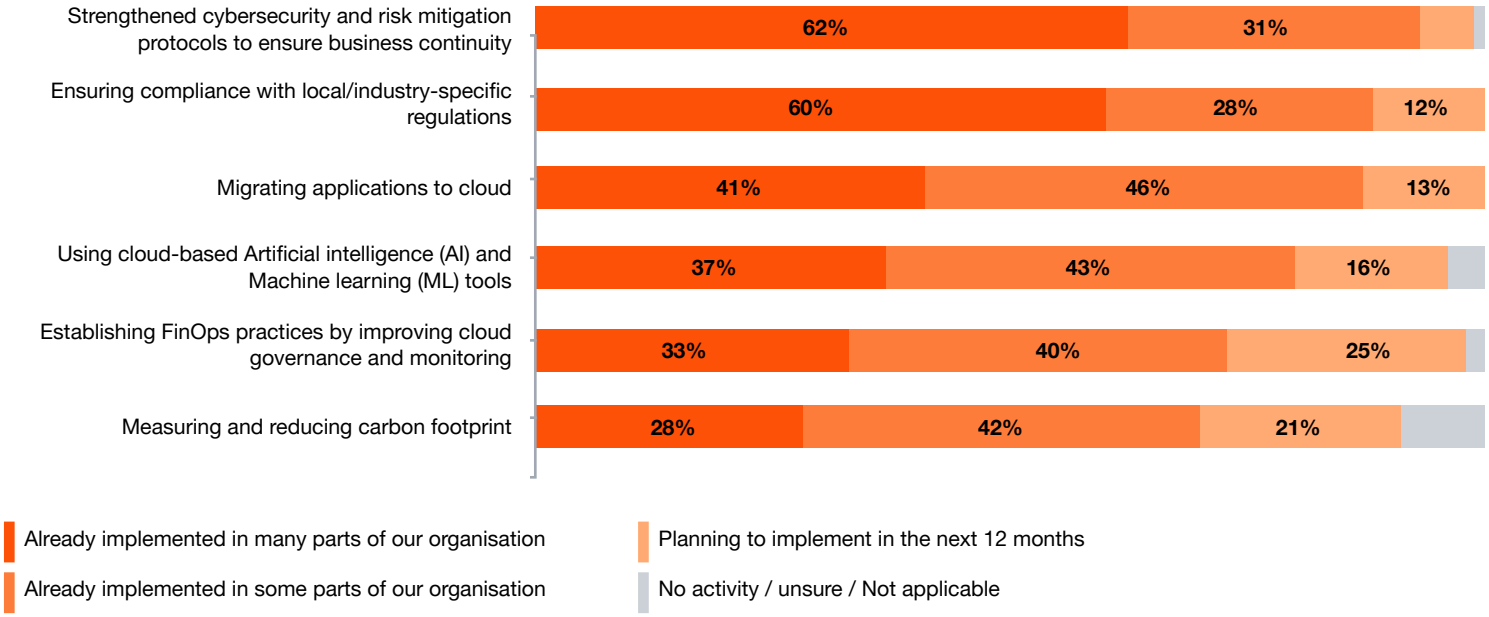
The strategic imperative

Organisations in Africa that accelerate enterprise-wide adoption—a core lever for efficiency, resilience, and innovation—will advance their digital transformation to deliver business value, building on the strong foundations already established across the continent.

The next value step is modernisation so applications can take advantage of elasticity, reliability and cost transparency. Africa's leadership in security and compliance, combined with broad application migration and early momentum in AI and ML, creates a solid platform for value creation. Organisations that now modernise migrated applications and industrialise AI, while keeping risk disciplines at the core, will convert adoption into measurable business outcomes.

Figure 2.

Which, if any, of the following cloud-related initiatives has your organisation implemented or is planning to implement?



Base: Africa respondents (162)

Source: PwC's EMEA Cloud Business Survey, September 2025

Beyond migration, progress is slow

A closer look reveals a more nuanced picture. Although cloud adoption is widespread across Africa, many organisations still struggle to progress from initial migration to full optimisation and cloud-native modernisation.

- Fewer than one in three organisations have modernised legacy systems across the enterprise, and only about half have managed to modernise in selected parts of their organisation.

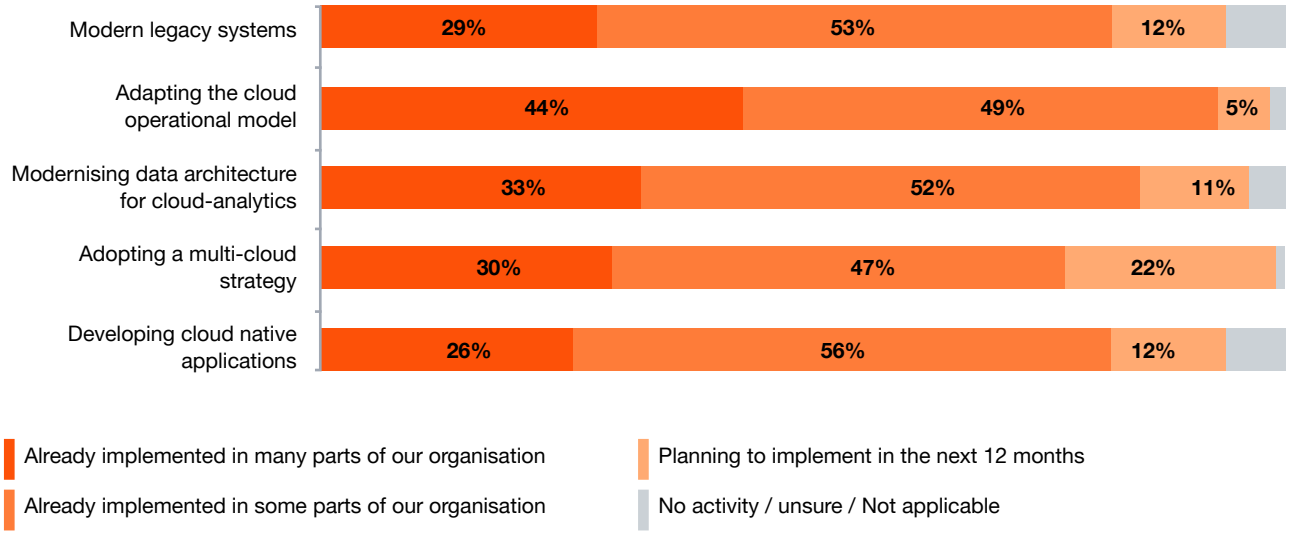
Technology leaders also highlight that execution of enterprise-wide cloud initiatives remains limited:

- Only 33% have modernised their data architecture to support cloud analytics across many areas of the organisation.
- Fewer than one in three have deployed multi-cloud strategies or rolled out cloud-native applications at scale.

Progress is more evident in foundational capabilities, with around 44% of organisations having adapted their cloud operating models across many parts of the organisation—an important step toward achieving long-term cloud maturity.

Figure 3.

Which, if any, of the following cloud-related initiatives has your organisation implemented or is planning to implement?



Base: Africa respondents (Technology – 73)

Source: PwC's EMEA Cloud Business Survey, September 2025

Case study: South Africa – integrated financial services group

Challenge: A leading South African insurer-bank faced escalating cloud costs after transitioning to the cloud, compounded by duplicate environments and sluggish change processes. These issues led to outages and unclear ownership, eroding trust and hindering AI investments while increasing regulatory and operational risks.

Approach: We collaborated to craft a comprehensive cloud operating model and governance framework. The team established a FinOps Centre of Excellence, revamped core customer and risk applications into microservices and event-driven architectures, and initiated a structured cloud/data academy for engineers, product managers, and risk/compliance teams.

Outcomes: With robust standards and skills in place, credit and fraud models transitioned from pilot to full-scale use. This shift reduced unit run costs, enhanced resilience, and accelerated release cycles.

Key insight: Architecture, governance, and talent should be viewed as a unified, long-term transformation. Achieving cloud maturity requires embedding technology change within the operating model, financial discipline, and capability building.

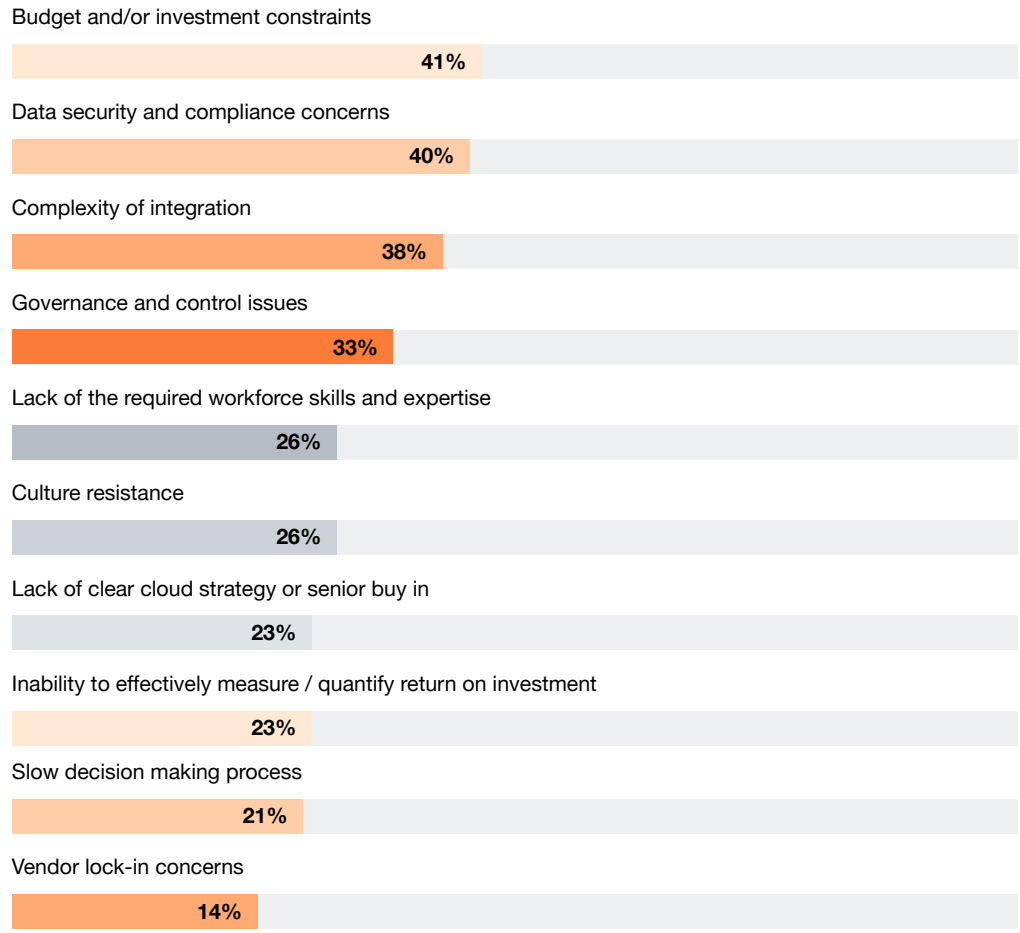
Internal barriers hold organisations back

Organisations in Africa are advancing in cloud adoption but face unique challenges that require specific solutions:

- **Budget pressures are more intense in Africa.** Nearly half (41%) of leaders in Africa say financial constraints block them from getting real business value from cloud investments—a higher rate than other EMEA regions. This reflects a broader global issue: 36% of CEOs in **PwC's 29th Global CEO Survey** worry they lack the capital to fund new initiatives that could improve operations.
- **Budget constraints have become the biggest internal roadblock to cloud success.** The solution requires focused IT investment and a cloud strategy that aligns with business goals. Yet 23% of leaders say they're missing either a clear strategy or support from senior management.
- **Security concerns slow down migration.** Some 40% of organisations in Africa cite data protection and compliance as major barriers, compared to 35% across EMEA. These worries affect both IT teams (41%) and business units (39%), often preventing systems from getting approved for cloud moves.
- **Unclear governance creates additional friction.** One-third of organisations in Africa struggle with cloud governance and control issues—higher than the 25% average across EMEA. When rules and responsibilities aren't clear, costs increase and security risks grow.
- **Skills gaps and complexity add to the challenge.** Finding and keeping talent is difficult for 39% of CEOs according to our **CEO Survey** data. Meanwhile, 38% of companies find integrating cloud solutions too complex, suggesting the need for simpler approaches and better-trained teams.

Figure 4.

Which, if any, are the biggest internal barriers to your organisation achieving measurable value from your cloud strategy?



Base: Africa respondents (162)

Source: PwC's EMEA Cloud Business Survey, September 2025

Investment momentum builds

Despite numerous challenges, there is a positive shift in Africa with strong planned investment momentum. Africa signals a decisive pivot toward AI, cybersecurity, and controls. Consistent with EMEA trends, 18% of organisations plan to increase cloud budgets by 15% or more, 36% plan increases of 6-14%, and 34% anticipate increases up to 5%, reflecting sustained investment in cloud-based strategies.

88%

of organisations plan to increase their cloud budgets in the year ahead, compared with 82% in 2023.

> Such a move–whether delivered incrementally through migration, modernisation, or the adoption of cloud-native technologies–requires significant business transformation and concentrated investment across multiple programmes. This helps explain why many organisations are increasing cloud spend, even as they work to realise clearer returns from AI and cloud initiatives. At the same time, the growing investment by hyperscale providers in Africa, through in-country presence and new local regions, is strengthening the cloud ecosystem. These developments support the momentum reflected in our survey and will be critical in helping organisations close the gap between ambition and measurable value.
>
> **Tshifhiwa Makhari**
> Cloud Leader, PwC South Africa

Leaders are prioritising investment in cloud controls, customer experience, and innovating new digital products and services. But top of the list is AI. Organisations in Africa have ambitious goals for AI implementation, with more than half of business and technology leaders (54%) looking to improve decision making and innovation as a measurable outcome from their investments. But business impact is often not realised. Results from our **CEO Survey** suggest significant implementation challenges. 66% of CEOs indicate that AI has had little to no impact on revenue in the last 12 months. Furthermore, only 26% of CEOs in Africa believe that their AI investment is sufficient to deliver their organisations' AI goals.

This disconnect raises important questions about AI implementation effectiveness. While leaders actively seek returns through better decision making, cost savings and new revenue streams, most aren't seeing tangible business impact. This suggests challenges around insufficient investment scale, ineffective implementation, or unrealistic ROI expectations.

What's next: AI in focus

AI is a top priority for cloud investment and is reshaping cloud decisions across Africa. The swift rise of cloud solutions, paired with AI advancements, is reshaping the strategic landscape across Africa. With AI as a key investment, the data highlights Africa's strategy to use cloud technologies for smart, sustainable growth.

46%

include AI in their top three investment priorities.

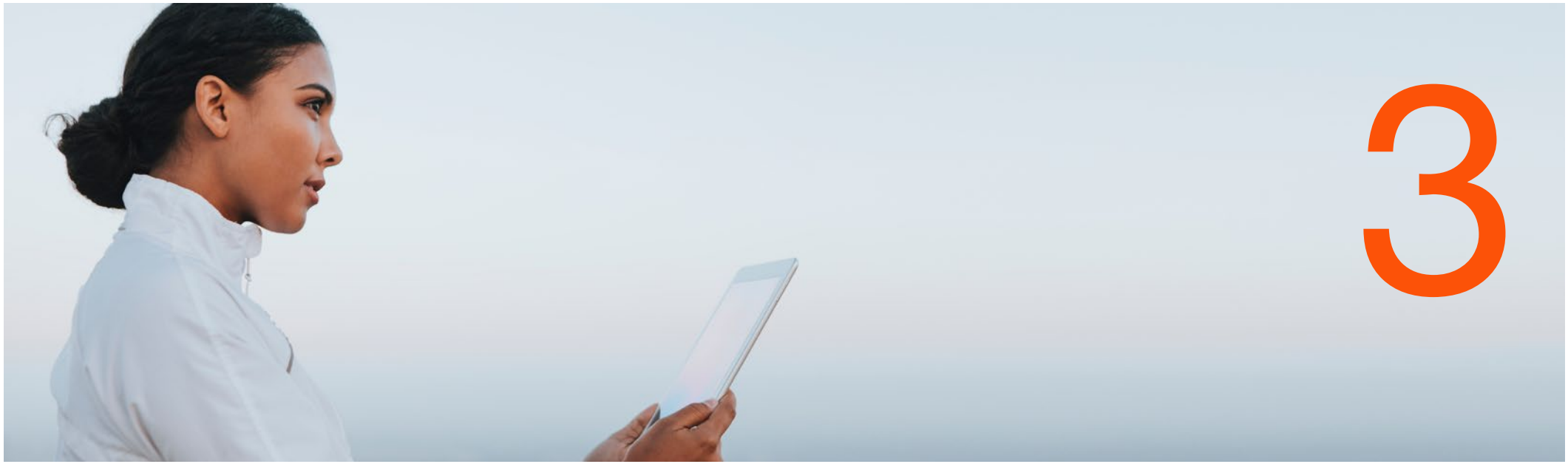
54%

prioritise improved decision-making outcomes from AI implementations.

> The rapid integration of cloud solutions with AI advancements is revolutionising Africa's business landscape, accelerating innovation and positioning the region as a pioneering leader in digital transformation and cutting-edge technology adoption. AI has evolved beyond an add-on to become the core driver of cloud investments in Africa, empowering businesses to achieve smarter decision-making and sustainable growth that will shape the continent's future economic landscape.
>
> **Laolu Akindele**
> Cloud Leader, PwC Kenya

Business and technology leaders across Africa are reshaping their cloud infrastructure to better harness emerging AI capabilities. Alongside this shift, organisations continue to prioritise cost optimisation, risk management, and improved performance—mirroring trends seen across EMEA. This demonstrates that AI-driven workloads are increasingly central to cloud architecture and design decisions on the continent.

Although AI adoption is rising, many organisations remain in early testing or pilot phases. Building the necessary workforce skills and strengthening data governance will be critical to scaling AI effectively and responsibly. As organisations in Africa continue to mature, external forces—such as regulation, geopolitical dynamics, and hyperscaler investments—are playing a growing role in shaping their next steps.



3

Geopolitics and regulation: The new cloud borders

Geopolitics and regulation are redefining the rules of cloud

Organisation in Africa have progressed from adoption to optimisation, but value realisation now hinges on external factors. Cloud value in Africa is shaped by geopolitics, regulation, and foreign exchange.

Cloud strategies are evolving:

89%

of organisations in Africa are refining their cloud approach in response to geopolitical and/or regulatory change.

> In this environment, realising cloud value depends on how effectively organisations respond to shifting geopolitical, regulatory, and economic pressures. Cloud strategies must be flexible enough to adapt to new compliance requirements, resilient to currency and cost fluctuations, and aligned to national sovereignty expectations. Those that proactively manage these external forces will be better positioned to unlock the full benefits of cloud and accelerate their transformation.

Mark Allderman
Africa Cloud and Digital Leader,
PwC South Africa

Redrawing the cloud map

Geopolitical tensions and evolving regulations are reshaping how data is stored, processed, and secured. Governments are mandating localisation and "sovereignty-by-design" models, requiring organisations to operate securely within regulated environments while maintaining control over sensitive data.

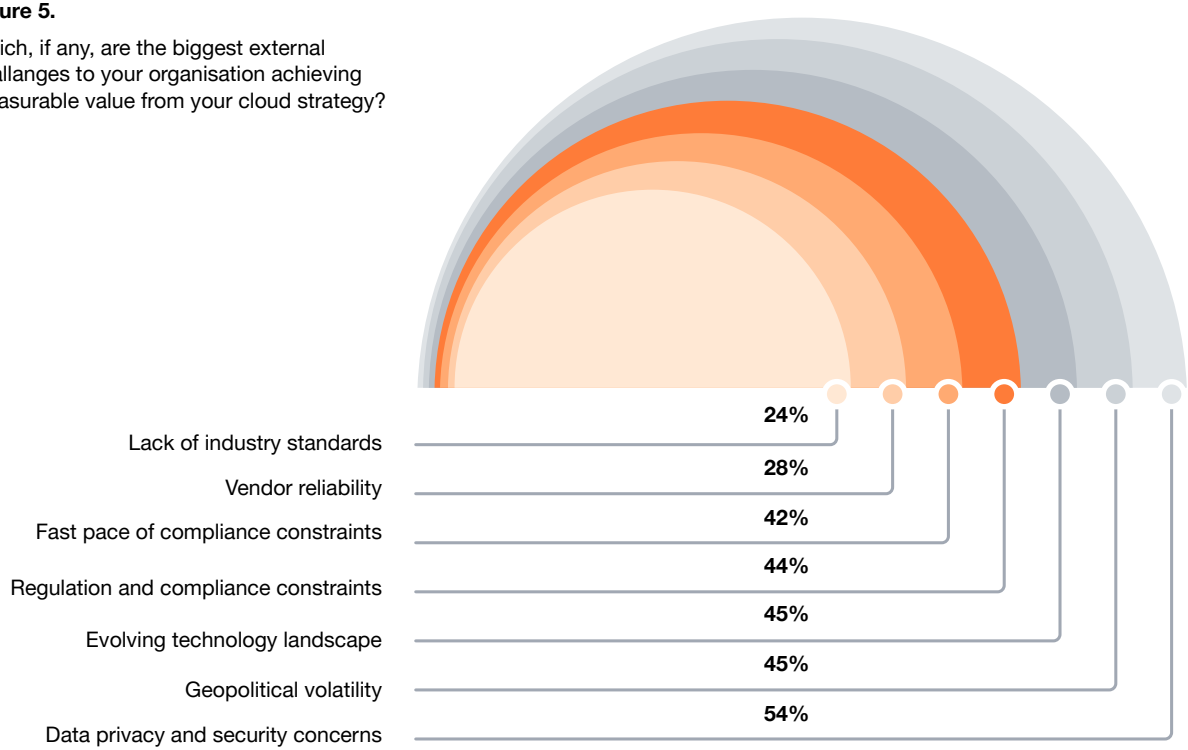
The cyber threat landscape is driving urgent action across Africa. According to our **CEO survey**, 29% of CEOs believe they are highly or extremely exposed to cyber risks, with 61% intending to continue enhancing enterprise-wide cybersecurity to defend against cyber-attacks as a result of geopolitical conflict over the next three years. This aligns with broader priorities, as data privacy and security rank at the top for business and technology leaders, while geopolitical shifts affect 45% of organisations in Africa, demanding flexible strategic planning.

Africa's varied regulatory landscape compounds these security imperatives, from South Africa's POPIA to Nigeria's NDPR and Kenya's Data Protection Act, necessitating adept compliance strategies.

Consequently, sovereign and hybrid cloud patterns are increasingly favoured to meet localisation requirements across diverse jurisdictions, especially in finance and healthcare sectors. Businesses in Africa must strategically align their cloud adoption with regional dynamics, investing in compliance frameworks and agile infrastructures to accelerate cloud maturity and build sustainable competitive advantage in the digital economy.

Figure 5.

Which, if any, are the biggest external challanges to your organisation achieving measurable value from your cloud strategy?



Base: Africa respondents (162)

Source: PwC's EMEA Cloud Business Survey, September 2025

Addressing Africa's four biggest external challenges:

Build compliance into delivery

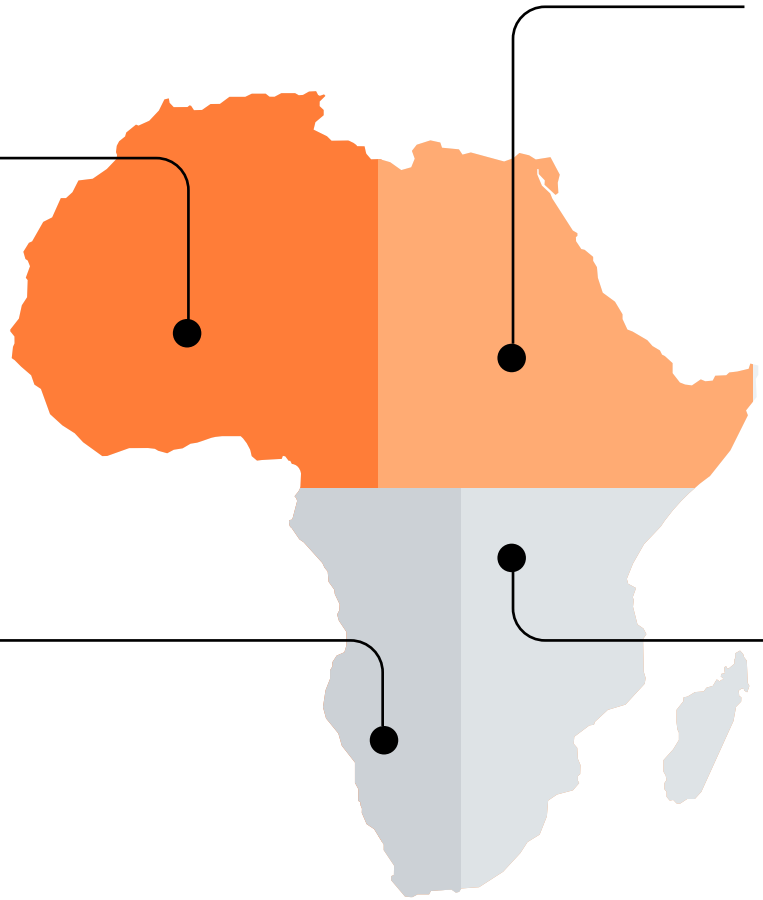
44%

require automated policy checks in build and release pipelines and map where data can legally reside before any migration. Target at least 90% of deployments with automated checks.

Design for geopolitical shocks

45%

run critical services in two regions and use country-resident hosting where needed. Limit any single-country exposure to 40% of critical workloads, with exit and failover clauses in provider contracts.



Security is the gate

54%

don't scale mission-critical workloads until core controls cover at least 95%: encrypt sensitive data at rest and in transit, verify every access request, and keep data in approved locations.

Stay ahead of technology change

45%

fund a Cloud Center of Excellence and standard, modular architectures (container-based patterns). Aim for 70% of workloads on approved patterns and 60% of engineers certified in core cloud skills.

Forex volatility stalls Africa's growth in cloud computing

Organisations in Africa face currency-driven cost fluctuations with USD-billed cloud services. To combat volatility in ZAR, NGN, and KES, organisations are bolstering FinOps and treasury strategies. Established cloud governance includes reserved capacity, egress reduction, and right–sizing to manage ongoing FX pressures.

Case study: Navigating FX volatility and cloud spend resilience in West and Southern Africa

Challenge: The fluctuating foreign exchange rates in Nigeria, Ghana, and South Africa have disrupted strategic plans, increased budgets, and weakened returns on investment.

Approach: We introduced a FinOps strategy that provides real-time visibility into FX rates, refines spending with local-currency tracking, optimises workload distribution, enhances contract terms, and employs treasury hedging.

Outcomes: We've seen a marked improvement in cost predictability and a boost in ROI. Cloud initiatives have regained their pace, bolstered by renewed confidence from leadership.

Key insight: It's crucial to design systems that focus on managing FX risks. By combining FinOps with financial controls and treasury strategies, we can drive continuous innovation even in volatile conditions.

Geopolitical pressures don't just require strategy shifts—they demand new infrastructure choices.

Currency volatility, evolving cross-border regulations, and shifting international alliances are pushing organisations in Africa to reconsider where and how their data and workloads are hosted. As a result, we're seeing accelerated demand for sovereign and trusted cloud solutions that offer greater control, regulatory alignment, and resilience against external disruptions.

Provider location and resilience matter

The choice of cloud provider location is critical, as geopolitical volatility and vendor reliability directly affect cloud resilience. Organisations should leverage in-country Providers and data residency options to minimise disruption and ensure compliance by diversifying energy sources, bolstering cybersecurity, and partnering with local tech firms.

Cross-border rules shape architecture

Regulatory environments shape cloud architecture. Compliance with the US CLOUD Act and African data protection laws requires embedding legal safeguards within contracts and technical infrastructure to ensure data protection across borders.

Data sovereignty is now a design choice

More organisations in Africa are directly addressing data sovereignty by choosing sovereign public cloud options for their potential in risk mitigation, security enhancement, and AI application, positioning these choices as integral to their cloud strategy.

US–South Africa relations remain a watchpoint

As international relations evolve, it's crucial to factor in trade and compliance considerations when utilising US-based cloud services in South Africa, ensuring prospective planning amidst political shifts.

Navigating cloud challenges in Africa: Strategic insights for resilience and success

Cloud storage realities differ widely across Africa, with each region facing unique challenges. We have studied these dynamics closely and are here to guide organisations through them.

South Africa

South Africa's electricity-supply instability, creates a need for diversified energy sources—such as solar, generators, and battery systems—to support resilient cloud and data-centre operations. In addition, stringent data-protection requirements call for strong security measures. Organisations must implement robust encryption and conduct regular security audits to meet the obligations of the Protection of Personal Information Act (POPIA). Leveraging local data-hosting capabilities further supports regulatory compliance, reduces latency, and enhances overall performance and user experience.

Kenya

Strengthening Kenya's technological infrastructure and cybersecurity requires close collaboration with local internet service providers to enhance network reliability and performance. Robust cybersecurity frameworks, supported by continuous staff training and awareness programmes, are essential for mitigating evolving threats. Adherence to the Data Protection Act further reinforces consumer trust by ensuring that personal data is managed and protected in line with regulatory requirements.

Nigeria

Nigeria faces a combination of geopolitical uncertainty and infrastructure limitations, making resilient cloud operations a strategic priority. Decentralising cloud environments helps reduce dependency on single data centres and strengthens continuity. Public–private partnerships play an important role in improving national infrastructure reliability, while maintaining regional data backups supports availability during periods of disruption. Compliance with the Nigeria Data Protection Regulation (NDPR) ensures that personal information is handled securely and in line with regulatory expectations.

4

Conclusion: Strategic choices must balance AI adoption with sovereignty and economic considerations

Turning cloud capability into competitive advantage

Strategic imperatives

Realising cloud's full potential requires addressing internal constraints—skills shortages, budget pressures, and legacy architectures–through focused strategic actions:

Invest in capabilities

Address skill gaps through targeted development, refine architectures, and deploy cost-effective solutions.

Engineer trust

Build secure, trustworthy environments from the outset to protect organisations and customers.

Modernise infrastructure

Re-engineer critical applications, retire non-value systems, and fix data quality at source.

Connect to outcomes

Translate cloud strategies into measurable results—speed, value, and resilience—supporting AI-driven demand.

Govern economics

Strengthen FinOps capabilities to ensure sustained value from cloud investments.

Build sovereignty

Place regulated workloads within national boundaries to meet compliance requirements while unlocking specific business value.

Success in this next phase will depend on organisations' ability to execute these strategic imperatives simultaneously—re-platforming cloud from a technology implementation into a comprehensive business platform that drives sustainable competitive advantage.

While resilient cloud foundations are essential for weathering geopolitical uncertainty, they're just the starting point. The next challenge lies in transforming this infrastructure into business value through intelligent automation, compliant sovereignty frameworks, and disciplined financial governance.

In part 2 of our report, "Beyond the foundation: Mastering AI, sovereignty and economics," explores how organisations are scaling AI capabilities, implementing sovereignty-by-design architectures, and governing cloud economics to turn investment into sustainable competitive advantage.

> As geopolitical tensions intersect with technological disruption, the contours of cyber threat are shifting. Sovereignty has become the north star for cloud strategy elevated to the top of policymaking, regulatory scrutiny and boardroom oversight. Most organisations are now undertaking a fundamental rethink of their cyber posture.

Vikas Sharma
Africa Cyber and Privacy Leader,
PwC Mauritius

Methodology

Region

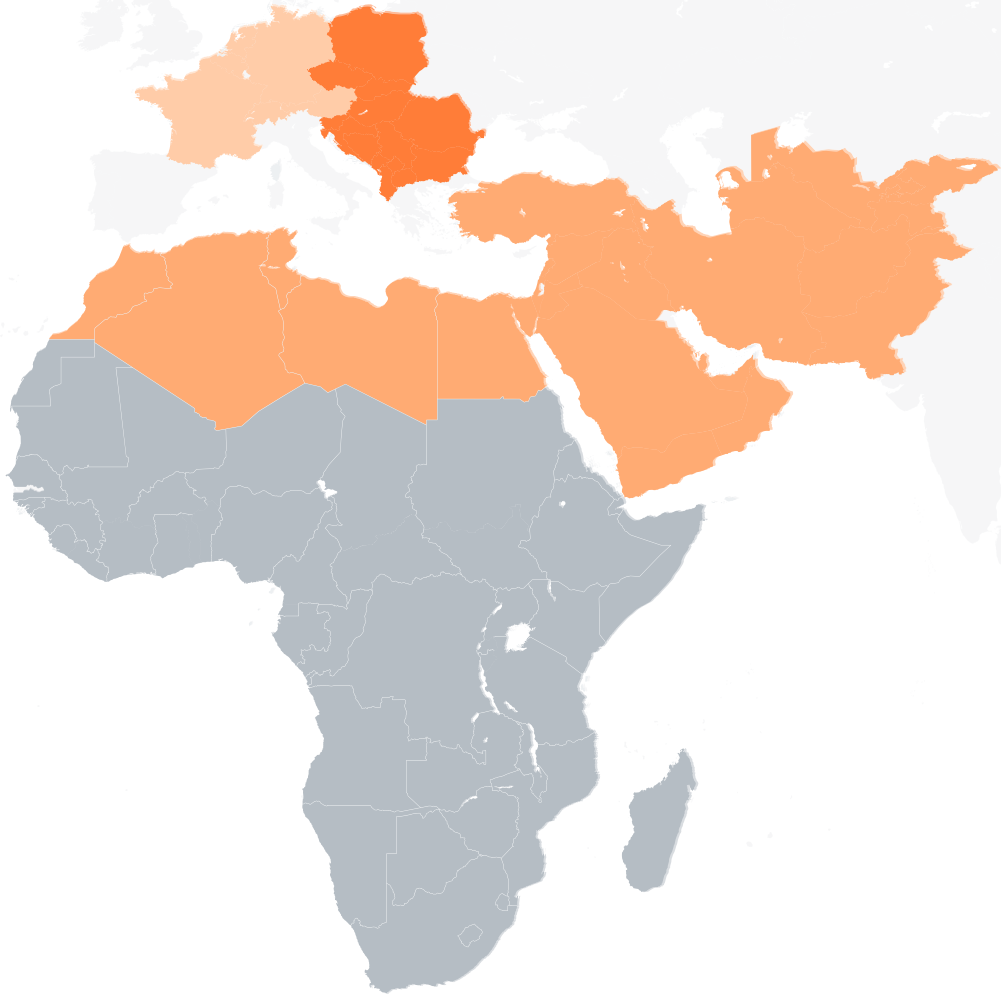
Between July and September 2025, PwC surveyed over 1,400 business and technology leaders across EMEA. Coverage across the EMEA regions:

54% Western Europe

20% Middle East

15% Central and Eastern Europe

11% Africa



Job role

Equal representation across business and technology leaders from C-suite and director roles:

- 50 % Business
- 50 % Technology

Revenue

56%

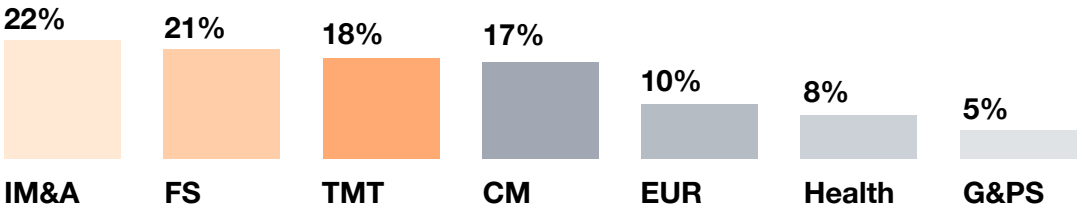
Less than US$1 billion

44%

From +US$1 billion

Industries

Respondents were from public and private companies in seven major industries:



Glossary

Cloud adoption:

the business-led move of the right apps and data into the cloud, along with new ways of working (skills, processes, governance) to get real value like speed, resilience, and clearer costs.

Cloud maturity:

how well cloud practices are embedded across the whole company—from strategy and architecture to security, operations, data, and finance—moving from ad hoc use to automated, measurable, outcome-driven ways of working.

Hybrid cloud:

integrates public and private cloud environments, allowing data and applications to move seamlessly between them for flexibility, scalability, and regulatory compliance.

Public cloud providers:

Global platforms such as Microsoft Azure, Google Cloud, Oracle Cloud, and AWS deliver scalable services across regions.

Managed service providers:

Operate and optimise cloud environments, often built on hyperscaler infrastructure but tailored to customer needs.

Sovereign public clouds:

Hyperscaler offerings (e.g. Microsoft Sovereign Cloud, Oracle EU Sovereign Cloud) combining local compliance with global innovation.

Trusted or national clouds:

Locally owned solutions (e.g. Delos Cloud, Bleu) serving government and critical infrastructure with isolated, compliant setups.

Private clouds:

Dedicated, on-premises or hosted environments (e.g. VMware Cloud, HPE GreenLake) offering maximum control but limited scalability.

GDPR:

The EU's General Data Protection Regulation sets strict rules on how organisations collect, process, and store personal data to protect individuals' privacy and rights.

NIS2:

The EU Network and Information Security Directive 2 strengthens cybersecurity requirements across critical and digital sectors, expanding scope and introducing stricter oversight and penalties.

DORA:

The Digital Operational Resilience Act establishes a harmonised framework for financial entities to withstand, respond to, and recover from ICT-related disruptions and cyber threats.

Cyber Resilience Act:

EU regulation setting cybersecurity standards for hardware and software products to ensure they are secure throughout their lifecycle and resilient to cyberattacks.

EU AI Act:

AI regulation that takes a risk-based approach to ensure AI systems are safe, transparent, and aligned with fundamental rights before entering the EU market.

Hyperscalers:

Large global cloud providers (e.g., Microsoft Azure, Google Cloud, AWS, Oracle Cloud) that offer massive scale, many services, and worldwide data centers.

Data residency:

where your data is stored and processed (country or region), often chosen to meet legal, performance, or customer trust needs.

Data sovereignty:

ensuring data follows a country's laws and control requirements, including who can access it and under what circumstances.

MTTD and MTTR:

Mean Time to Detect (MTTD) is how long it takes to spot a problem; Mean Time to Respond (MTTR) is how long it takes to fix it—both are key resilience metrics.

POPIA (South Africa):

Protection of Personal Information Act—South Africa's data privacy law setting rules for collecting, using, and protecting personal data.

Data Protection Impact Assessment (DPIA):

a risk assessment that checks privacy impacts before launching higher-risk data processing or AI projects.

MLOps (Machine Learning Operations):

the processes and tooling to train, deploy, monitor, and update AI models safely and reliably.

SOC (Security Operations Center):

a team and platform that monitors for threats and responds to incidents, often 24/7.

SIEM (Security Information and Event Management):

software that collects and analyses security logs to detect suspicious activity.

SOAR (Security Orchestration, Automation, and Response):

tools that automate security workflows and responses, often integrated with SIEM and SOC.

Agentic AI:

AI systems that can plan and take actions with limited human input, adapting to new data to complete complex tasks.

Generative AI:

AI that creates content (text, images, code) from patterns learned in training data.

Contacts

Hannelie Lotz
Principal, Cloud and Digital – Data,
PwC South Africa

Sameer Chetty
Associate Director,
Cloud and Digital,
PwC South Africa

Femi Madariola
Cloud Leader,
PwC Nigeria

Laolu Akindele
Cloud Leader,
Pwc Kenya

Vikas Sharma
Africa Cyber and
Privacy Leader,
PwC Mauritius

Junaid Amra
Cyber Leader,
PwC South Africa

Winston Anderson
Associate Director,
Cloud and Digital - Public Sector,
PwC South Africa

Jesse Twum-Boafo
Associate Director,
Cloud and Digital,
PwC South Africa

Mark Allderman
Africa Cloud and
Digital Leader,
PwC South Africa

Tshifhiwa Makhari
Cloud Leader,
PwC South Africa

Christiaan Nel
AI Africa Leader,
PwC South Africa

Andrew Dalling
Strategy& Fit
for Growth Leader,
PwC South Africa

Lilian Tilley-Gyado
Senior Manager,
Cloud and Infrastructure ,
PwC Nigeria

At PwC, we help clients build trust and reinvent so they can turn complexity into competitive advantage. We're a tech-forward, people-empowered network with more than 364,000 people in 136 countries and 137 territories. Across audit and assurance, tax and legal, deals and consulting, we help clients build, accelerate, and sustain momentum. Find out more at www.pwc.co.za
PwC South Africa refers to the South Africa group of member firms and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.