April, 2025
White Paper

Balancing Innovation and Compliance in the AI Era

Core42 Sovereign Public Cloud Leveraging Microsoft Azure

core42
A G42 company

Microsoft

Table of Contents

Executive Summary

Over the past two decades, the UAE has emerged as a global technology powerhouse, pioneering advancements in artificial intelligence (AI), cloud computing, and digital infrastructure. The nation has now set its sights on the future with ambitious plans to lead the next wave of digital transformation, with bold AI strategies, building world-class data centres, and investing heavily in cutting-edge technologies that will redefine industries and accelerate economic growth.

Cloud services have become the backbone of AI-driven digital transformation, providing organizations with the capacity, scalability, and agility needed to innovate. Yet, highly regulated sectors, such as government, banking, healthcare, and oil and gas, remain cautious about adopting public cloud solutions due to concerns over data sovereignty, security, and regulatory compliance, forcing them to walk a fine line between regulatory adherence and innovation.

Sovereign clouds offer a compelling solution to this challenge by maintaining data residency and compliance within specific national borders. Yet, traditional private cloud-based sovereign cloud solutions often limit organizations' ability to innovate at scale. This is where public cloud-based sovereign cloud solutions emerge as a game changer.

The Core42 Sovereign Public Cloud combines powerful Microsoft Azure hyperscale capabilities with UAE-specific sovereign and security controls, leveraging Core42's "Insight" platform to deliver a secure, compliant, and innovation-ready cloud environment tailor-made for the UAE's regulated sectors.

This white paper dives into the transformative role that sovereign enabled public cloud solutions play in shaping the UAE's digital future. It provides strategic insights and best practices for technology leaders to adopt and deploy these solutions effectively.

Key Takeaways

The UAE is doubling down on AI and cloud investments to drive its digital future.

Data sovereignty is mission-critical, with national regulations driving demand for secure cloud and AI solutions.

Sovereign enabled public clouds take a novel approach to providing data sovereignty, breaking the tradeoff between compliance and innovation, making them the ideal choice for regulated industries.

AI and Cloud: Powering UAE's Digital Future

Over the past two decades, the UAE has cemented its status as a global tech leader, evolving into one of the fastest-growing hubs for innovation. Leading organizations across the nation have embraced digital-first strategies, integrating cutting-edge technology into every aspect of their operations. This transformation has unlocked new revenue streams, streamlined processes, and boosted efficiency – all powered by strategic investments in AI and cloud, which are redefining industries and fueling sustainable growth.

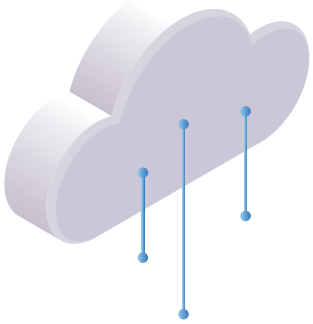
As the global AI race intensifies, the UAE has solidified its position as a frontrunner. The nation's AI-driven future is bold, first-of-their-kind initiatives, such as the appointment of the world's first AI minister in 2017, the launch of the world's first AI university in 2020, the development of large language models (LLMs) like Jais and Falcon, and the establishment of AI-ready data centers. The government itself is setting the benchmark for AI adoption, with AbuDhabi's Dh13 billion strategy to become the world's first fully AI-native government by 2027, and Dubai appointing 22 Chief Artificial Intelligence Officers (CAIOs) across key government entities.

But AI doesn't operate in isolation—it thrives in the cloud. Cloud services provide the scalability, agility, and capacity to fuel AI-driven transformation. Whether for powering applications through Infrastructure-as-a-Service (IaaS), developing solutions in Platform-as-a-Service (PaaS) environments, or leveraging AI-infused Software-as-a-Service (SaaS) applications, the cloud is the critical foundation for unlocking AI's full potential.

The momentum is undeniable. IDC reports that AI and Cloud are the top two technology investment areas for UAE organizations in 2025. Organizations increasingly turn to the cloud to build, train, and deploy AI models, whether through embedded AI functionalities in SaaS applications, or custom-built AI solutions.

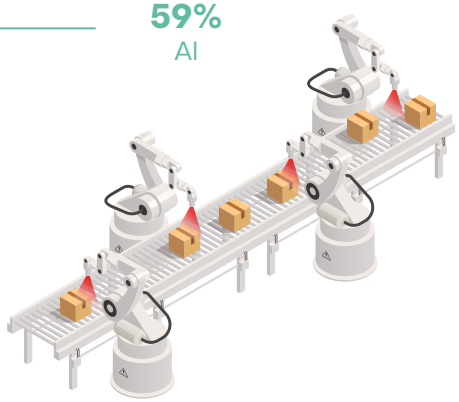
Figure 1: AI and Cloud are Top Priorities for UAE Organizations

52%
Cloud

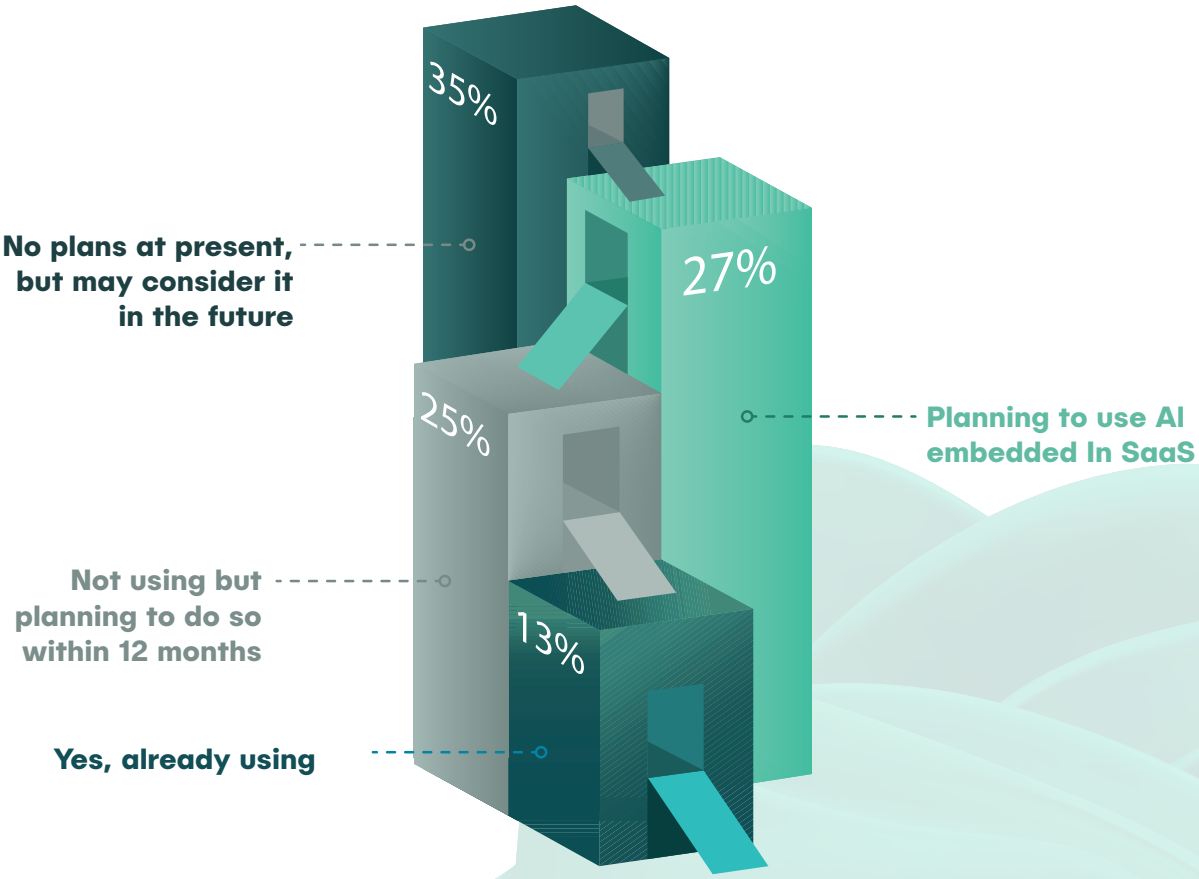


Top Areas Prioritized for Digital Technology Investments in 2025

59%
AI



UAE Organizations' Plans to Build AI Solutions on Cloud



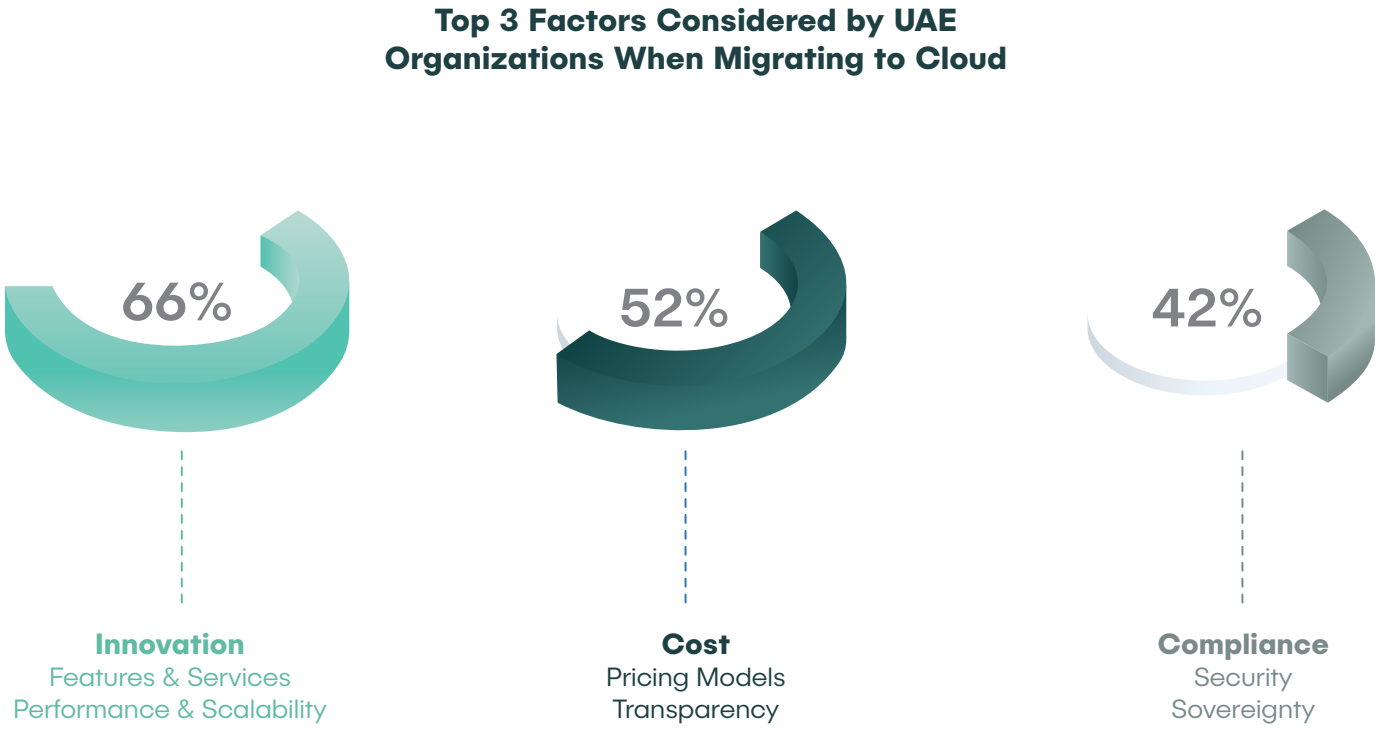
Source: IDC Digital Executive Sentiment Survey December 2024 (N=100, UAE, 250+ employees); IDC Cloud Survey October 2024 (N=100, UAE, 100+ employees).

Balancing Innovation and Compliance through Cloud

UAE organizations are rapidly embracing the cloud as the core technology platform, drawn by its ability to deliver cutting-edge innovations, unparalleled agility, and reduced IT burden. With hyperscaler investments in local cloud regions, a surge in indigenous cloud providers, and evolving regulations, adoption is skyrocketing. UAE public cloud spending hit $2.95 billion in 2024 and is set to soar to $6.47 billion by 2028, growing at a staggering CAGR of 21.7% as per IDC.

While organizations in non-regulated industries are rapidly adopting public cloud, regulated sectors, such as government, banking, healthcare, public utilities, national critical infrastructure, oil and gas, and others, remain cautious. Data sovereignty, security, and compliance concerns have kept them tethered to private clouds, which partially address their needs for scalability and control, but lack the full potential of public cloud-based innovation.

Figure 2: Balancing Innovation and Compliance is a Key Challenge



Source: IDC Cloud Survey October 2024 (N=100, UAE, 100+ employees).

As cloud adoption accelerates, organizations in regulated sectors need solutions that don't force them to choose between compliance and innovation. They need a cloud model that blends the best of both worlds - the scalability and innovation of the public cloud, along with the control, compliance, and security of the private cloud.

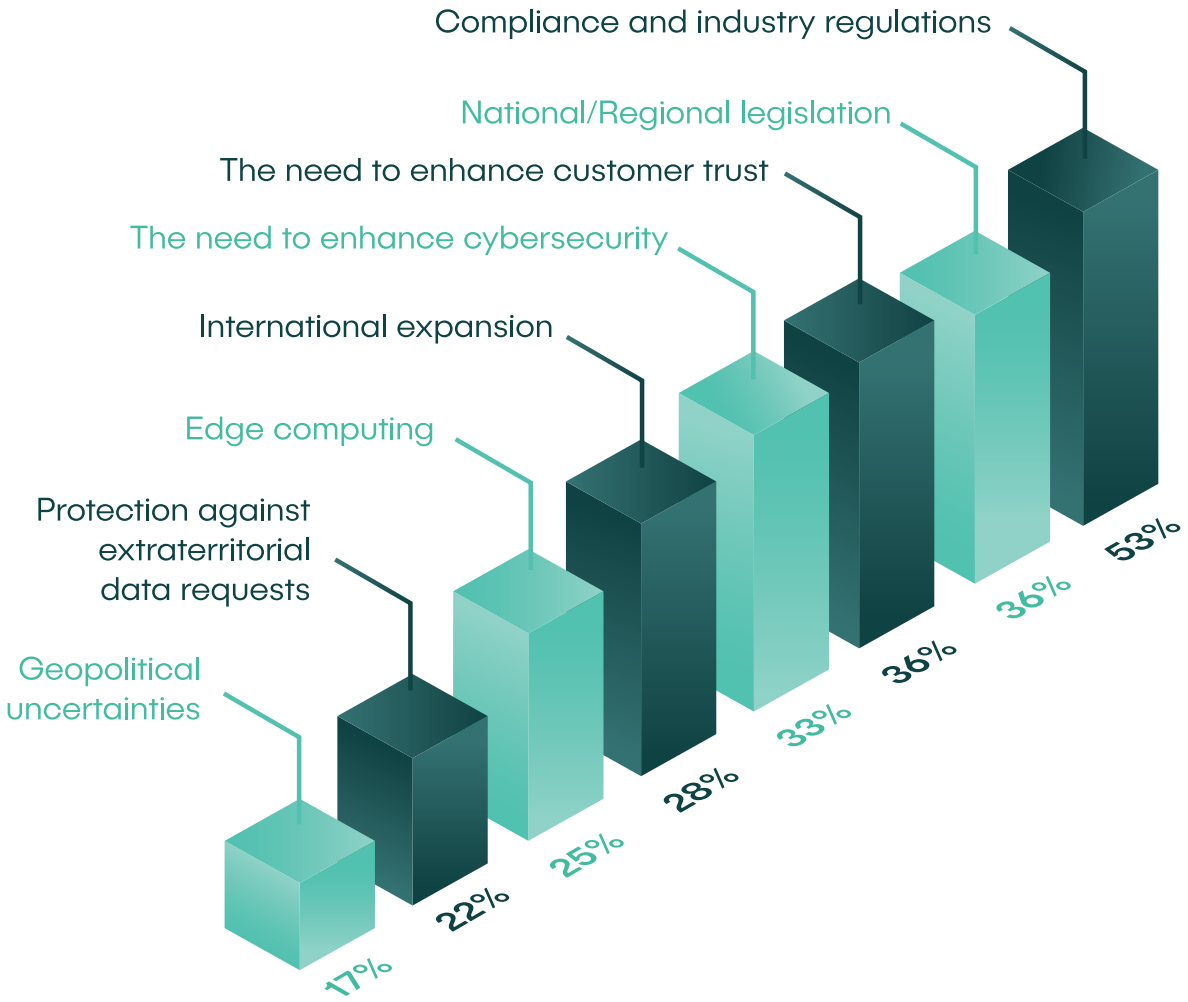
Maintaining Data Sovereignty in Cloud Adoption

With the rise of the digital economy, data has become a key strategic asset. As organizations and nations recognize its strategic value, data sovereignty has become a top priority, ensuring that data is governed by the laws of the country in which it is collected or processed. This means strict control over data privacy, security, localization, and cross-border flows, particularly for sensitive information.

The UAE has been at the forefront of this movement. In 2019, the UAE took an important step toward data sovereignty with its 'Smart Data Framework,' which stipulated that all entities treat data as a collective national asset and act as custodians. Since then, various laws such as the Personal Data Protection Law (PDPL) of 2021, as well as sector-specific regulations that govern health data and financial data, have reinforced the growing importance of data sovereignty in the country. Meanwhile, tech-specific strategies and policies, such as the National Cybersecurity Strategy and the National Cloud Security Policy, ensure that the nation's technological infrastructure remains protected.

The increasing adoption of AI further accelerates the importance of data sovereignty. With AI-driven systems relying heavily on vast datasets, ensuring these systems and their underlying data adhere to data sovereignty principles becomes critical. As AI adoption accelerates, so does the need for sovereign enabled public cloud solutions that give organizations the freedom to innovate without compromising security, compliance, or national data control.

Figure 3: What Drives Sovereign Cloud Demand in the UAE?



Source: IDC Cloud Survey October 2024 (N=100, UAE, 100+ employees).

Addressing Data Sovereignty Needs

A sovereign cloud is designed to maintain data residency, compliance, and control within a specific country or region with the main objective to protect data against extraterritorial jurisdiction such as the Cloud ACT to maintain data sovereignty which refers to the concept that data is subject to the laws and governance of the country in which it is collected, stored, or processed. This is particularly critical for governments and regulated industries that must comply with national and sector-specific regulations to ensure data security, privacy, and compliance.

In recent years, sovereign cloud solutions have rapidly evolved driven by shifting regulatory landscapes, growing investments in local cloud infrastructure, and expanding global-local cloud partnerships.

Two Models of Sovereignty in Cloud: Private vs. Public

Sovereign cloud solutions come in two primary flavors: private cloud which is typically a disconnected environment and sovereign enabled public clouds, which are relatively a new paradigm. These models differ mainly in how they achieve sovereignty and at what levels, defined by factors such as data sovereignty and residency, operational sovereignty and technology sovereignty.

Public cloud

Public clouds with various new technical and policy control features have recently begun to offer governments and regulated entities solutions to help, enable them to harness hyperscale cloud services while maintaining compliance with national and sector-specific sovereignty regulations.

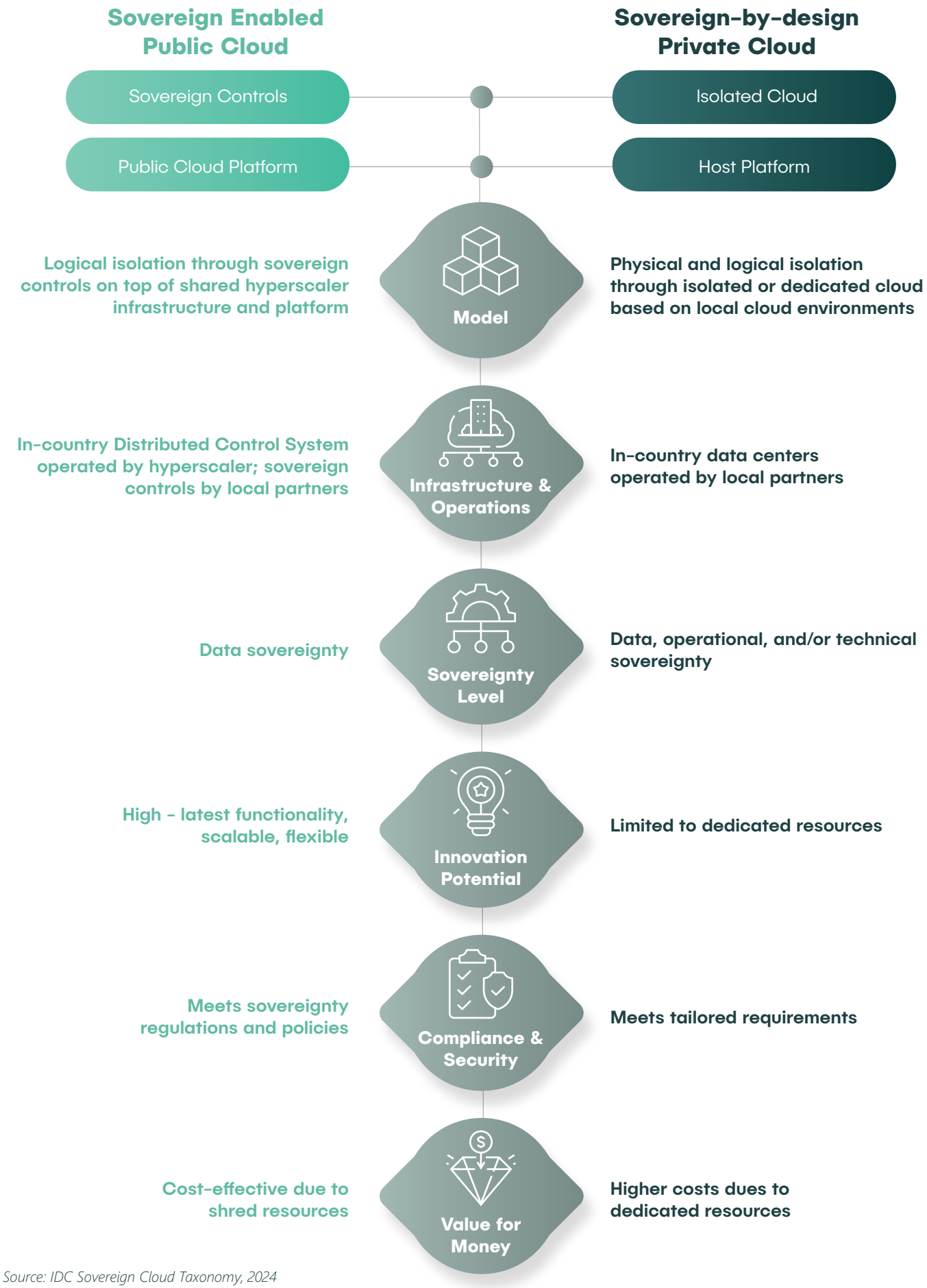
This model integrates regulatory assurance mechanisms, such as data residency enforcement, sovereign technical controls, encryption (at rest, in transit, and in use), and policy-based access management, to ensure that data is governed under local jurisdiction. By deploying sovereign controls, public cloud platforms can align with national security and compliance requirements while still benefiting from scalability, cost efficiency, and cloud-native innovations. This approach is well-suited for regulated industries such as healthcare, financial services, and government entities that need to maintain data sovereignty without sacrificing the flexibility and innovation of public cloud services.

Private cloud

Private clouds offer a disconnected (often referred to as air-gapped) or restricted connectivity cloud which is a fully isolated cloud environment designed to ensure that sensitive data remains within a specific jurisdiction, accessible only by authorized entities.

These environments operate independently from the global internet and public cloud infrastructure, enforcing strict security measures such as dedicated infrastructure, physical separation, and stringent access controls. Air-gapped sovereign clouds are often used by government agencies, defense and critical industries that require the highest level of security, regulatory compliance, and operational sovereignty. This model guarantees that no external entity, including foreign cloud providers, can access or influence the data, making it ideal for handling classified information, sensitive workloads, and highly regulated industry data.

Figure 4: Sovereign Cloud Deployment Models



Source: IDC Sovereign Cloud Taxonomy, 2024

Advantages of Sovereign Enabled Public Cloud

The sovereign enabled public cloud strikes a balance between innovation and compliance, addressing key challenges that organizations in regulated sectors often face with cloud adoption. By leveraging the global public cloud provider's platform and the local provider's expertise, this model offers a scalable sovereign cloud environment for organizations while maintaining complete regulatory control. Key features and advantages of sovereign enabled public cloud include:

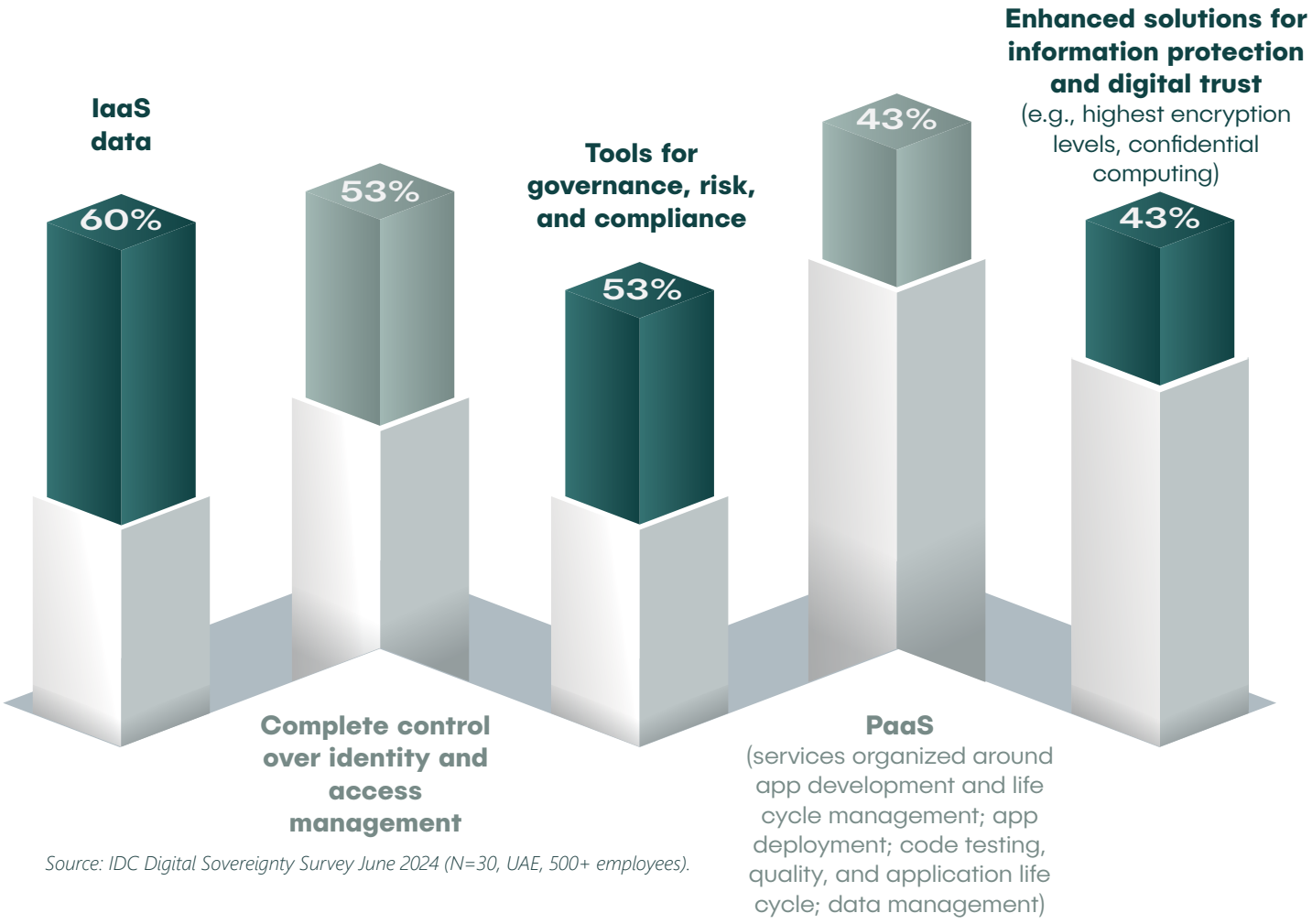
In-country data centers to ensure data residency.

Sovereign controls managed by a local partner prevent unauthorized access and enforce regulatory compliance, while pre-built policy packs simplify complex regulatory requirements.

Shared model and its OPEX-based pay-as-you-go options, make it cost-effective and adaptable for organizations of all sizes.

Advanced capabilities make the latest technological innovations (such as GenAI) easily accessible in a scalable environment, delivering agility, faster time-to-market, and a future-proof infrastructure.

Figure 5: Sovereign Cloud Deployment Models

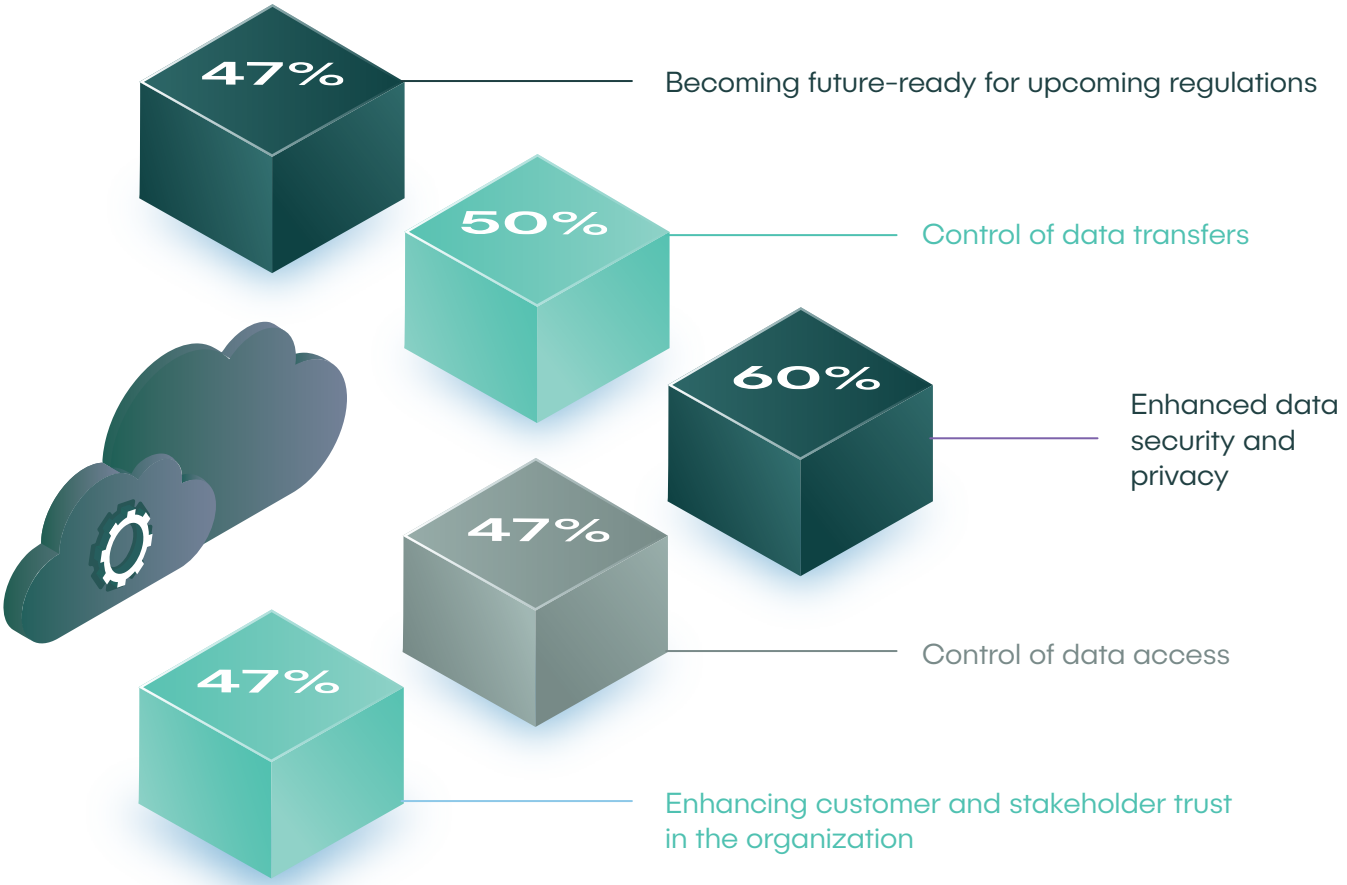


Source: IDC Digital Sovereignty Survey June 2024 (N=30, UAE, 500+ employees).

Organizations in heavily regulated sectors, such as finance, government, healthcare, and energy, are the primary adopters of sovereign cloud services. However, the demand is rising fast as organizations across industries increasingly seek to enhance regulatory compliance, gain greater control over data, and strengthen their cybersecurity posture.

Sovereign enabled public cloud solutions significantly improve an organization's security with built-in features such as advanced encryption processes, confidential computing, and strict guardrails. These measures help mitigate the risks associated with cybersecurity breaches and data leaks. Beyond avoiding massive fines from regulators, a single data breach can cripple an organization's reputation for years. Sovereign enabled public cloud solutions mitigate risks while enabling businesses to remain compliant, resilient, and future-ready.

Figure 6: How Organizations in the UAE Benefit from the Sovereign Enabled Public Cloud?



Source: IDC Digital Sovereignty Survey June 2024 (N=30, UAE, 500+ employees).

Sovereign Enabled Public Cloud for Regulated Industries

Banking & Finance

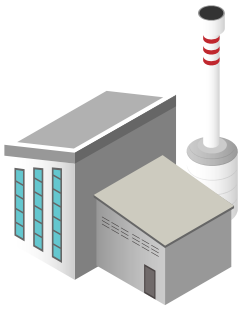
Organizations in the banking and finance sector operate under the stringent regulations set by the Central Bank of the UAE (CBUAE), Abu Dhabi Global Market (ADGM), and Dubai International Financial Centre (DIFC). With data residency, security, and operational continuity at the core of compliance mandates, financial institutions must ensure that critical workloads such as core banking systems and payment processing run on highly available, secure, and compliant infrastructure. At the same time, the sector's competitive nature demands rapid and continuous innovation in digital banking and AI-driven services.

Sovereign enabled public cloud solutions present an optimal solution enabling financial institutions to process and store data within UAE-based cloud infrastructure while accessing the latest technological advancements. Compliance features such as pre-built policy packs, audit logs, and robust access controls simplify adherence to regulatory requirements. These solutions also drive digital transformation by enabling digital-first delivery models, AI-powered customer experiences, and fraud detection mechanisms. Furthermore, as the financial sector embraces open banking initiatives, sovereign enabled public cloud offers a secure and efficient platform for collaboration between banks and fintechs that fosters innovation while maintaining compliance.

Government

UAE's ambitious initiatives, including Abu Dhabi's AI-native government strategy and Dubai's Universal AI Blueprint, demonstrate a strong commitment to leveraging AI to enhance public services, streamline operations, and improve governance. At the same time, government agencies manage vast amounts of sensitive data, ranging from citizen records and national security intelligence to critical infrastructure assets, making adopting new technologies challenging. Sectors such as defense, law enforcement, and citizen services require strict compliance and sovereignty requirements. Additionally, national strategic objectives, such as fostering in-country value creation, further influence the organization's approach to IT infrastructure.

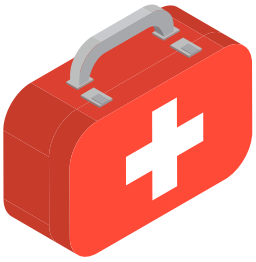
Sovereign enabled public cloud solutions address these challenges by providing a secure and compliant environment for governments to modernize digital services without compromising data sovereignty. The localized infrastructure ensures that sensitive government data remains within the UAE, safeguarding national interests while promoting innovation in public sector delivery. The solution enables advanced cybersecurity measures, secure citizen data management, the seamless integration of digital identity services, and the rapid adoption of technologies like AI, IoT, and big data analytics for more effective public sector operations. interests while promoting innovation in public sector delivery.



Oil & Gas

Organizations in the oil and gas sector conduct large-scale operations, generating massive datasets from remote and geographically dispersed locations such as offshore rigs and extensive pipeline networks. This includes geological survey and exploration data, production records, and financial information—all highly sensitive and subject to strict national regulations. The industry requires IT environments capable of real-time data analysis, that ensure high availability, and strong protection against increasing cyber threats.

Sovereign enabled public cloud solutions address these challenges by offering a secure and resilient infrastructure tailored to the industry's needs. The secure localized infrastructure coupled with access to cutting-edge technologies enables real-time analysis of large datasets, unlocking capabilities like predictive maintenance, supply chain optimization, and advanced geological modeling. Compliance with national regulations is seamlessly integrated, allowing for secure data sharing among key stakeholders, including government regulators and international partners. Furthermore, the adoption of AI and IoT within sovereign cloud environments drives operational efficiency and enhances decision-making, positioning the oil and gas sector for sustainable growth.



Healthcare

The healthcare sector handles sensitive patient data, requiring strict adherence to local regulations such as the UAE Healthcare Data Law, and in some cases, international standards like HIPAA and GDPR. Electronic health records (EHRs), medical imaging, and public health data must be securely stored and processed while ensuring seamless interoperability across national platforms such as Dubai's Nabidh and Abu Dhabi's Malaffi. As the sector increasingly adopts AI and big data analytics for diagnostics, research, and disease management, the need for a cloud environment that balances compliance with innovation becomes critical.

Sovereign enabled public clouds provide healthcare organizations with a scalable, compliant digital infrastructure. By ensuring that patient data is stored and processed within UAE borders, the solution meets the strict national and international requirements on data residency and security. The encryption, access controls, and secure data-sharing capabilities protect against breaches or unauthorized access while enabling interoperability. Furthermore, AI-driven public health initiatives, powered by sovereign cloud platforms, enable predictive analytics for disease surveillance, personalized treatment plans, and real-time healthcare insights, driving better patient outcomes while maintaining regulatory compliance.

Best Practices in Migrating to Sovereign Enabled Public Cloud

Migrating to a sovereign enabled public cloud isn't just about moving workloads — it's about maintaining compliance, security, and long-term operational success, even during the migration process. A strategic, well-executed approach minimizes risks and maximizes the benefits of a secure, scalable, and regulation-ready cloud environment.

The first step is a comprehensive assessment of the current infrastructure, data, and workloads to determine the compliance requirements and the right cloud model. Establishing clear success metrics for the migration and the sovereign enabled public cloud operational environment is crucial for a smooth transition and sustainable operations. Choosing the right sovereign enabled public cloud provider that meets the organization's unique regulatory and data sovereignty needs, security priorities, and digital transformation goals is equally crucial. This section outlines best practices across key stages of migration, ensuring organizations can navigate complexity while unlocking the full potential of a sovereign enabled public cloud solution.

Figure 7: Migration Approach to Implementing Sovereign Enabled Public Cloud

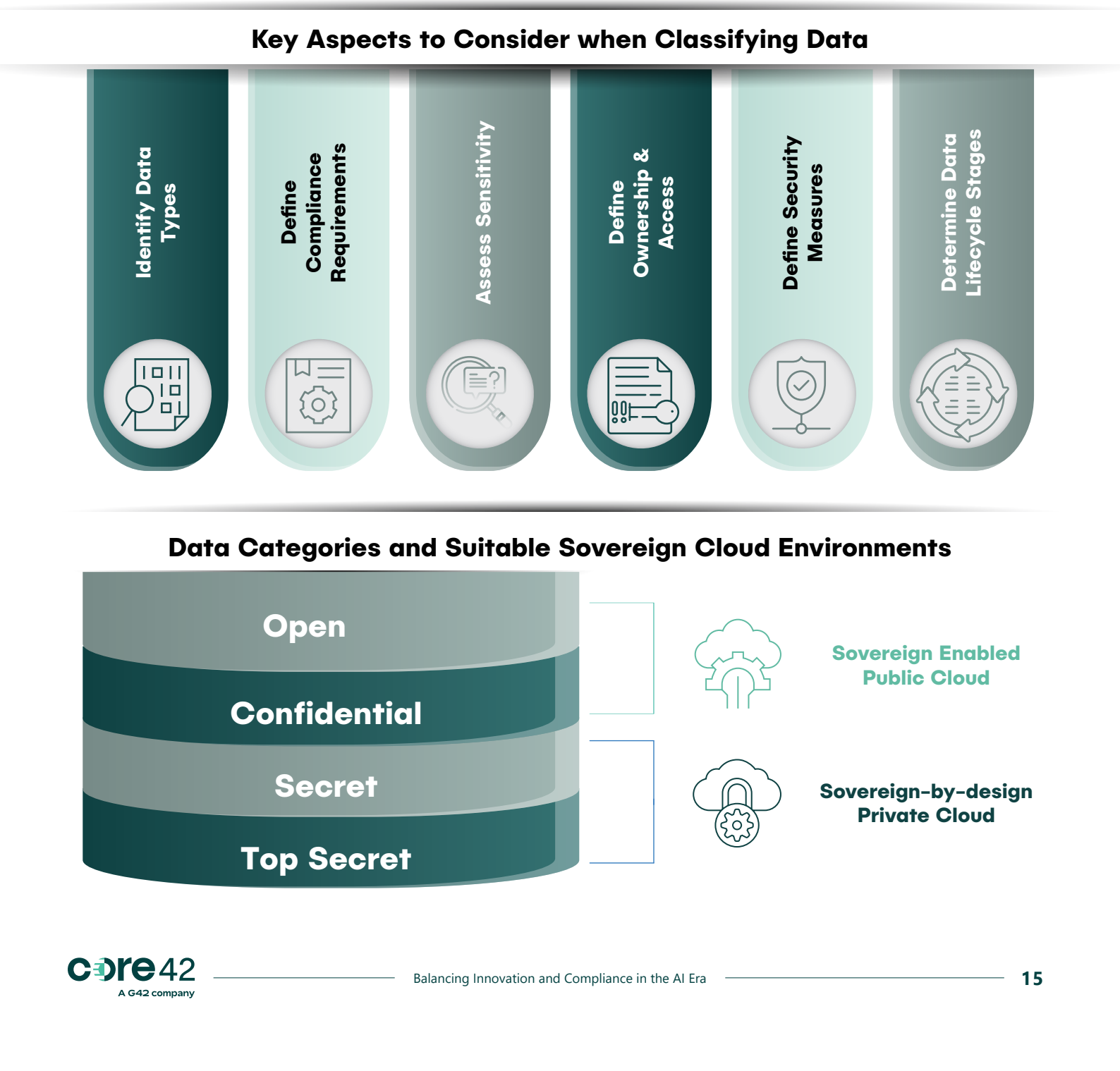
Classifying Data & Choosing the Right Cloud

Data classification plays a pivotal role in determining the appropriate sovereign cloud model. The UAE Smart Data Framework[1] , established by the Telecommunications and Digital Government Regulatory Authority (TDRA), categorizes data into four levels: open, confidential, secret, and top secret. This classification is based on various factors, such as the nature of the data, its sensitivity, compliance and security requirements, ownership, access needs, and stage in the data lifecycle.

For workloads with open and non-sensitive data, a public cloud may be viable, especially for non-regulated sectors. However, organizations in regulated sectors dealing with open and confidential data require a sovereign enabled public cloud that balances compliance, security, and interoperability. With workloads that handle secret and top secret data that demand absolute control, the sovereign-by-design private cloud, with hardware isolation and operational sovereignty, becomes the optimal choice. Aligning the storage, processing, and security of data and workloads with regulatory mandates and organizational policies through this classification-driven approach maintains compliance and unlocks cloud-powered innovation.

[1]*https://u.ae/en/about-the-uae/digital-uae/data/data-operability*

Figure 8: Classifying Data & Choosing the Right Sovereign Cloud Model

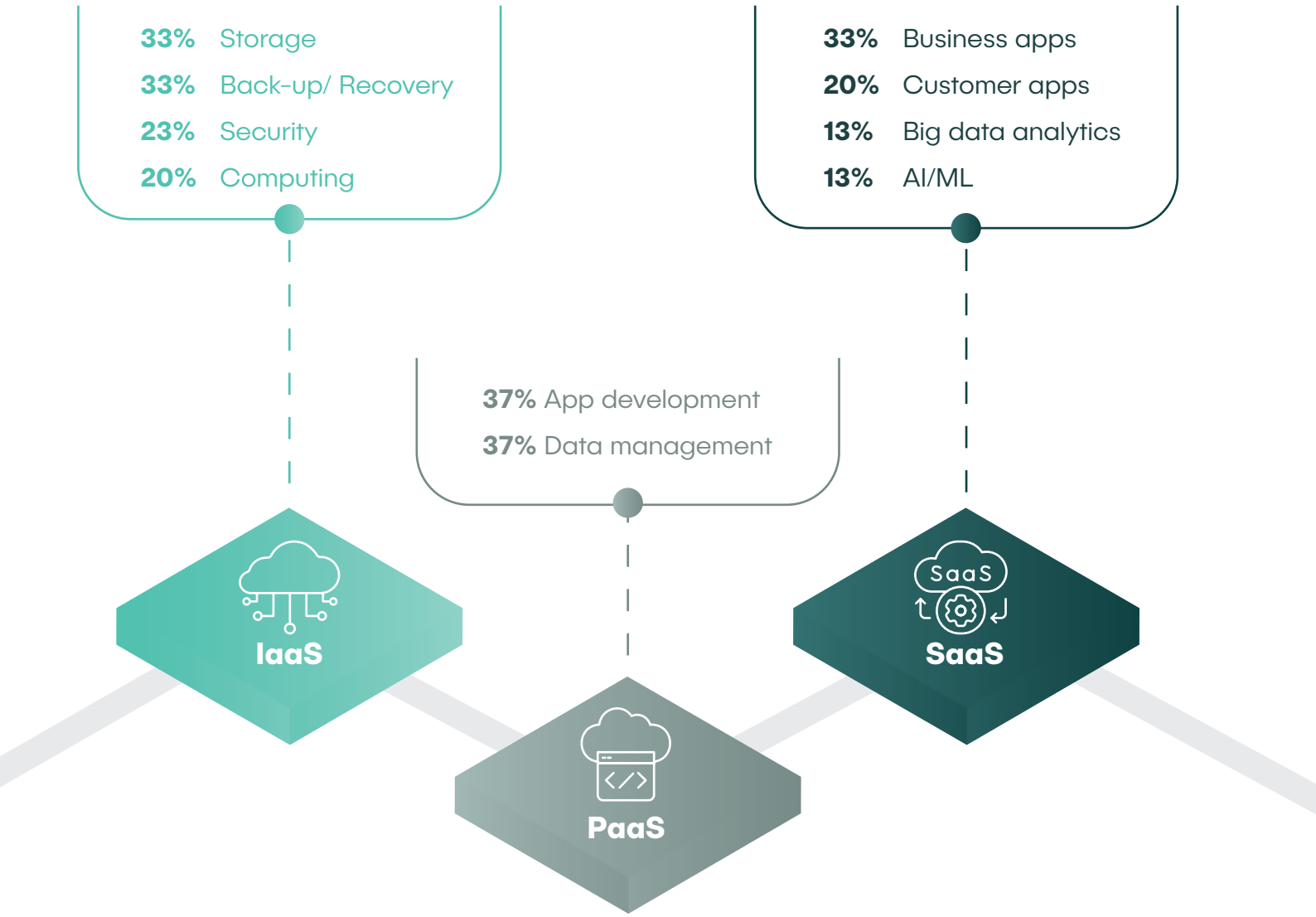


Choosing the Workloads for Sovereign Enabled Public Cloud Migration

After classifying data, organizations must determine which workloads should move to the sovereign enabled public cloud. The decision depends on local regulations, applicable legislation, and the sensitivity of the data involved.

Many enterprises start with foundational workloads such as backup, data storage, and security applications before gradually transitioning into workloads supporting digital transformation—such as application development, data management, core applications, analytics, and AI. This phased approach enables organizations to scale securely while maintaining compliance.

Figure 9: Which Workloads are UAE Organizations Migrating to Sovereign Cloud?



Source: IDC Digital Sovereignty Survey June 2024 (N=30, UAE, 500+ employees).

Measuring the Success of Migration and Effectiveness of Sovereign Enabled Public Cloud

In a hybrid multicloud environment, it is critical to measure the effectiveness of the environment continuously. Organizations must establish Key Performance Indicators (KPIs) to monitor the performance, security, cost efficiency, and regulatory adherence of the sovereign enabled public cloud environment. From uptime and latency metrics to data sovereignty compliance and cost optimization, these KPIs help organizations maintain operational resilience while adapting to evolving regulations.

Figure 10: KPIs to Measure the Effectiveness of Sovereign Enabled Public Cloud

Choosing the Right Sovereign Enabled Public Cloud Provider

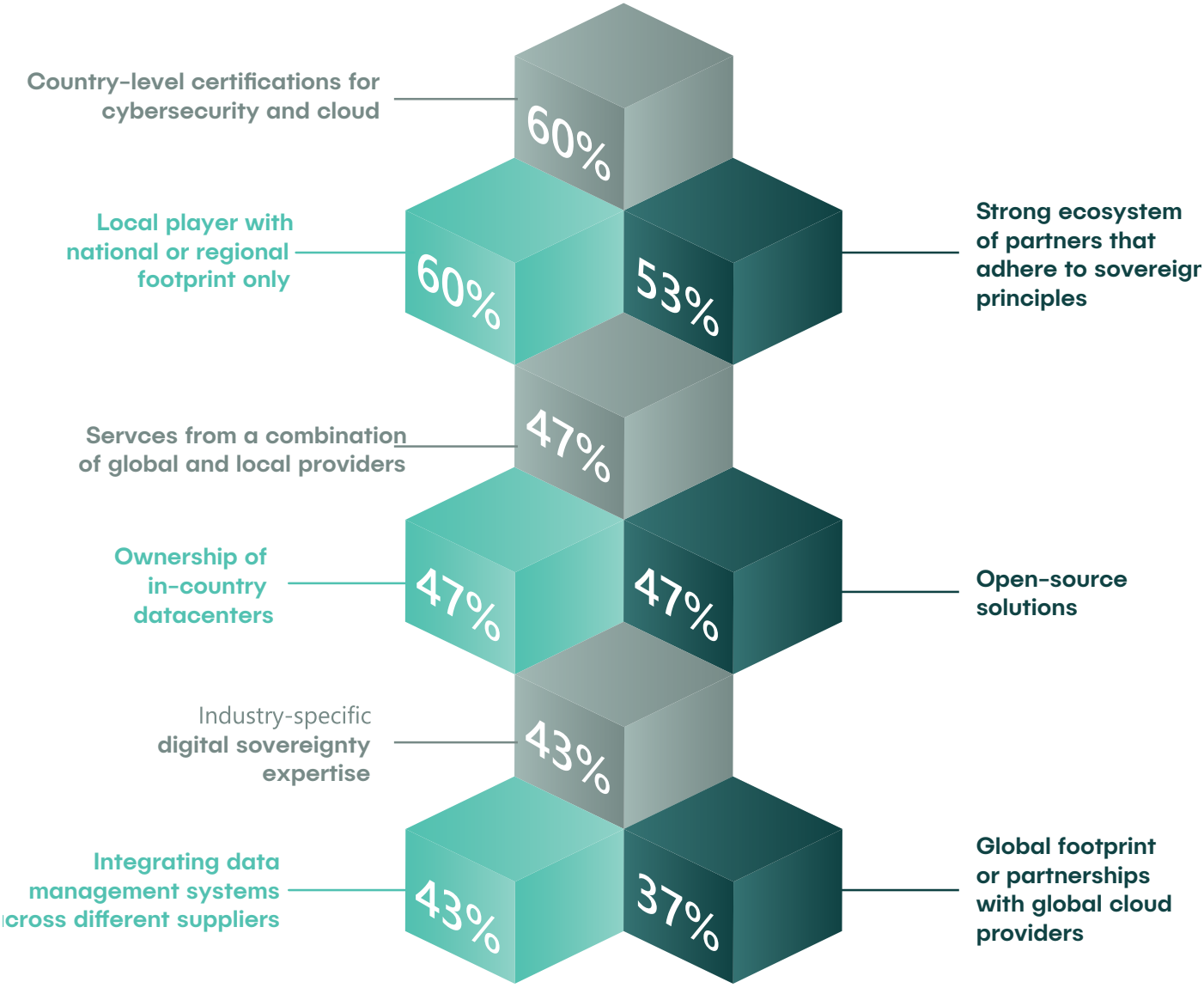
Choosing the right sovereign enabled public cloud provider is about more than infrastructure—it's about finding a partner that delivers both compliance and innovation at scale. A trusted sovereign cloud model relies on a global cloud provider with extensive scalability, AI capabilities, and innovation pipelines paired with a local cloud partner that maintains regulatory compliance, market expertise, and national data control.

When assessing the global cloud provider, organizations should consider the core infrastructure capabilities, including availability, latency, scalability, and reliability. Additionally, their solution portfolio's breadth and depth, an extensive partner ecosystem, and the availability of skilled resources are essential indicators of their capabilities. Innovation remains a crucial consideration, so evaluating the provider's AI capabilities and roadmap is vital. Furthermore, industry-specific solutions and sustainability initiatives should also be considered when selecting a provider that aligns with the organization's broader strategic goals.

For the local partner, sovereignty credentials take center stage. Alignment with UAE national policies, engagement with policymakers, and deep expertise in compliance frameworks are crucial. Additionally, their ability to provide services such as system integration, skills training, and technology consulting is critical to ensure a smooth and efficient cloud transition and seamless operation.

Beyond individual capabilities, the synergy between the global provider and the local partner is critical. A shared vision for sovereignty, security, and innovation, along with a long-term commitment to compliance-driven cloud solutions, sets the foundation for a resilient and future-proof sovereign enabled public cloud solution. By carefully evaluating the providers and their collaborative relationship, organizations can confidently adopt a sovereign enabled public cloud solution fueling digital transformation while protecting national and organizational data sovereignty.

Figure 11: What UAE Organizations are looking for in a Sovereign Enabled Cloud Provider



Source: IDC Digital Sovereignty Survey June 2024 (N=30, UAE, 500+ employees).

Core42 Sovereign Public Cloud – Leveraging Microsoft Azure

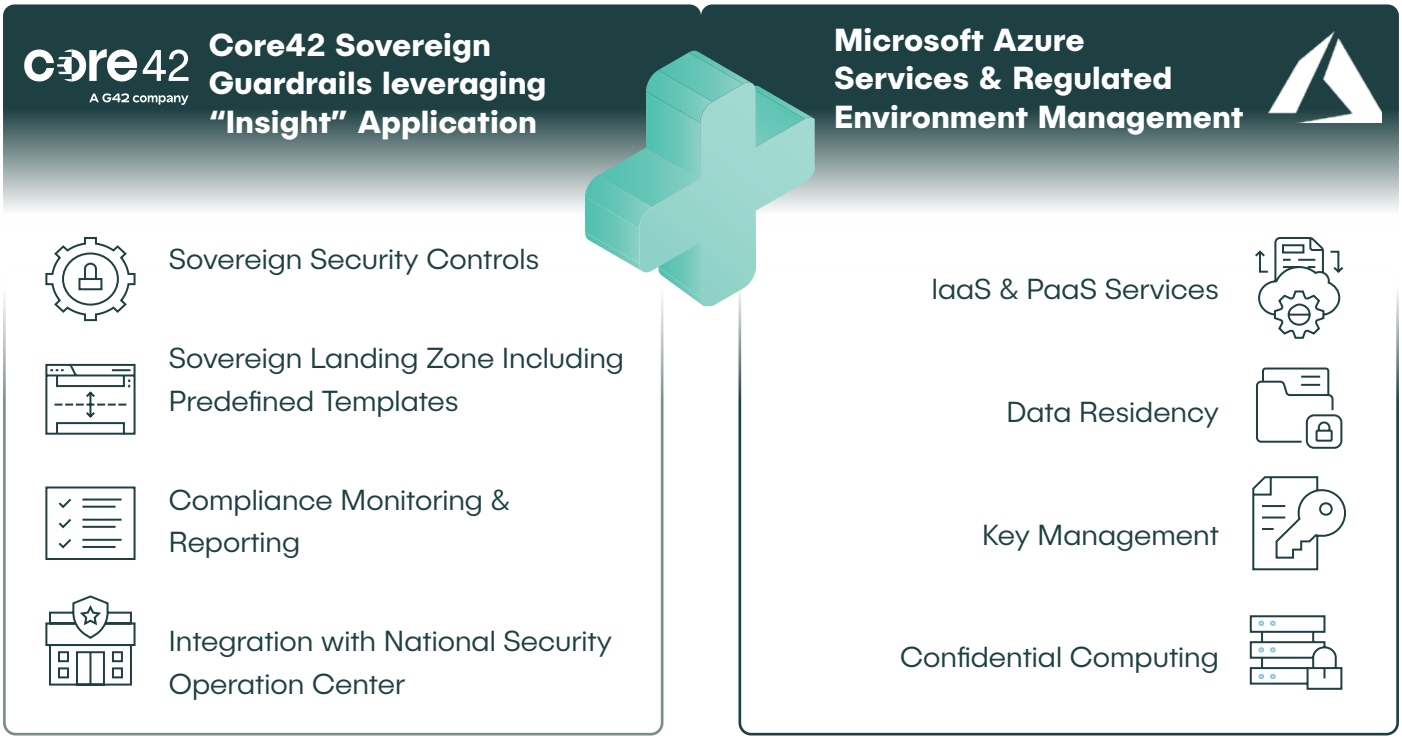
Core42, a digital infrastructure provider under the G42 group, is redefining sovereign cloud solutions in the UAE. Core42's Sovereign Public Cloud combines powerful Microsoft Azure hyperscale capabilities with UAE-specific sovereign and security controls leveraging Core42's Insight application, enabling government entities and regulated industries in the UAE to accelerate digital transformation while maintaining the highest standards of data residency, compliance, and security.

G42 and Microsoft joined forces in 2023 to expand the data center infrastructure and jointly develop sovereign public cloud offerings and AI capabilities for the UAE. The collaboration empowers entities in the UAE public sector and regulated industries to harness the functionality and feature set of Azure's cloud and AI technologies while maintaining data sovereignty, security, and compliance with local privacy laws and regulatory mandates.

Key Features of the Solution

Core42's Sovereign Public Cloud provides a game-changing solution for government and regulated entities in the UAE. By combining the innovation and scalability of Microsoft Azure's hyperscale infrastructure with Core42's pre-built sovereign and security controls leveraging Core42's Insight application, entities can adopt next-generation cloud technologies without compromising regulatory compliance.

Figure 12: Overview and Features of the Solution



The versatile SaaS-based Insight application combined with Microsoft's Azure cloud platform streamlines compliance through key features such as role-based access, logical isolation, and advanced security. Organizations maintain complete control and authority over data storage, processing, and access, all while leveraging the scalability, flexibility, and advanced capabilities of Azure's public cloud.

Core42's comprehensive policy library provides access to national and sector-specific regulatory frameworks making compliance simpler, faster, and more efficient. Features such as compliance evaluations, drift analysis, scheduled reports, custom alerts, and actionable recommendations provide organizations with unparalleled visibility and control over their cloud operations. Additionally, the platform includes robust monitoring for activity logging, SOC integration, and incident response which further enhance security by detecting and addressing malicious behavior.

Why Choose the Core42 Sovereign Public Cloud

Core42's strategic partnership with Microsoft offers the best of both worlds: Azure's cutting-edge innovation and scalability, paired with Core42's Insight application along with deep expertise in compliance, sovereignty, and local regulations. Core42's strong understanding of the UAE market dynamics and local regulations enable clients to remain compliant with national regulations while staying ahead of evolving requirements. Leveraging Microsoft's global leadership in technological advancements, particularly in AI, organizations can realize the use cases faster, accelerating digital transformation. This unique model also enhances cloud operations by seamlessly integrating with the Azure ecosystem, simplifying governance, and automating sovereign controls, thus reducing the technical burden on IT teams.

Figure 13: Key Value Proposition of the Solution

Accelerated Innovation

- Access to the full suite of Azure's products; AI, big data, and IoT
- Scalable infrastructure

Advanced Compliance

- Pre-configured sovereign controls aligned with local and global regulations
- Regular updates, real-time monitoring, Automated enforcement, and reporting

Advanced Security

- Access to confidential computing, encryption and key management
- Advanced threat detection and incident response

Optimized Resources

- Seamless integration with Azure
- Low operational complexity for IT teams

Competitive Advantages of the Core42 Sovereign Public Cloud

The Core42 Sovereign Public Cloud delivers a unique value proposition by integrating Core42's sovereign controls with Microsoft Azure's hyperscale infrastructure. This makes it a niche product in the UAE market, providing the solution a distinct competitive advantage in the sovereign cloud space.

At the heart of this offering is the strategic partnership between Core42 and Microsoft, which brings together best- in-class capabilities. Core42, a UAE-born company and a key entity within the G42 ecosystem, contributes deep local expertise, regulatory alignment, and integration across G42's extensive network of companies.

Core42's sovereignty & security offering deeply aligns with the UAE regulatory requirements and its role in building AI-optimized infrastructure and localized AI models further strengthens its ability to serve government & regulated industries. It provides customers with a regulatory advantage, helping them meet complex compliance requirements while advancing their digital transformation agendas.

Microsoft, meanwhile, brings global public cloud and AI enablement services to the table. A 2024 independent third-party study across 1954 end user organizations in the EMEA region provides significant insights into Microsoft's dominance in the cloud arena. In this study, the end-user organizations ranked Microsoft Azure as the best-in-class cloud provider in sovereignty and seven other attributes. Additionally, Azure was ranked similar to the closest competitor in five additional attributes.

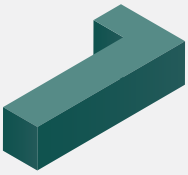
Figure 14: Global Cloud Providers Ranked Across Key Attributes

Source: An independent study conducted in 2024 by a leading global research firm, surveying decision-makers from 1,954 end-user organizations across EMEA

As the UAE continues its rapid digital transformation, the Core42 Sovereign Public Cloud, leveraging Microsoft's hyperscale capabilities with Core42's deep-rooted local expertise, is setting the standard for secure, compliant, and scalable cloud solutions—enabling organizations to innovate without compromise.

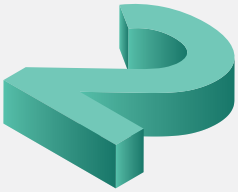
Outlook & Essential Guidance for Tech Buyers

Today, digital sovereignty is a strategic necessity and a vital business requirement for organizations in regulated sectors. The momentum behind the sovereign cloud is undeniable. Global spending on sovereign cloud solutions is set to nearly double in just three years, with IDC forecasting an increase from $133 billion in 2024 to $259 billion by 2027—a staggering CAGR of 26.6%. This surge reflects the growing need for data control, regulatory compliance, and operational resilience. In a data-driven era, ensuring operational integrity and strategic autonomy requires organizations in regulated sectors to take key actions:



Incorporate Sovereignty into Strategy

Stay informed about evolving regulatory frameworks and recognize the strategic importance of sovereignty at both organizational, sectoral, and national levels. Incorporate sovereignty into your technology strategy, enterprise architecture, procurement, and operations.

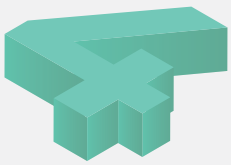


Assess and Prioritize Workloads

Conduct a comprehensive assessment of your workloads and categorize them based on data sensitivity and operational criticality. Prioritize workloads accordingly to move them to Sovereign Public Cloud.

Embrace Cutting-Edge Solutions

Explore emerging options, such as Sovereign Public Cloud, which offers novel approaches to address the limitations of existing solutions while ensuring compliance and security requirements specific to the sector – government, finance, healthcare, or other regulated sectors.



Consider the Cloud Lifecycle

Evaluate Sovereign Public Cloud solutions with a focus on the cloud lifecycle - from workload creation to its retirement. Ensure the solution supports seamless operations and efficient management throughout its lifecycle.

Select Providers Strategically

Opt for providers offering sovereign public cloud solutions that combine world-class capabilities and roadmap with local and industry-specific needs. Choose a partner committed to the UAE's long-term goals and aligned with the nation's and industry's vision for digital sovereignty.

By taking these strategic steps, organizations in regulated sectors can lead the charge in a sovereignty-first digital economy—maintaining compliance, resilience, and innovation without compromise.