



Sovereign Cloud

Intelligent Boundaries for Accelerated Innovation



An IDC White Paper

Author: Jebin George, Senior Research Manager, IDC
June, 2025

In partnership with



Executive Summary

As digital transformation accelerates across industries, the ability to control data, infrastructure, and digital operations within national borders has become a critical imperative. Digital sovereignty, once a regulatory consideration, is now a strategic enabler of innovation, security, and resilience.

In the UAE, this shift is particularly pronounced. With a growing number of organisations adopting digital-first strategies, and national authorities enforcing robust data protection and cloud security frameworks, the need for sovereign cloud solutions has never been greater. Sovereign clouds enable organisations to meet stringent regulatory requirements, safeguard sensitive data, and maintain operational control, — all while benefiting from the flexibility and scalability of modern cloud technologies.



At the same time, emerging technologies such as artificial intelligence (AI) are creating new sovereignty concerns. Organisations are increasingly seeking sovereign AI capabilities that align with national policies and ensure responsible use of sensitive data. The integration of sovereignty principles into AI strategies is no longer optional, — it is essential for building public trust and long-term viability.

This whitepaper examines the rising importance of digital sovereignty, with a focus on the UAE's evolving regulatory environment and national data protection priorities. It provides a foundational understanding of sovereign cloud principles, outlines key deployment models, and presents the core technology requirements that enable data, technical, and operational sovereignty. The document also explores common adoption challenges, best practices for implementation, and critical success factors. Additionally, it offers guidance on selecting the right sovereign cloud partner, —based on transparency, compliance capability, ecosystem maturity, and local governance.

The whitepaper also highlights the architecture and features of the du Sovereign Cloud built on Oracle Alloy, showcasing how this solution empowers innovation while safeguarding national digital interests. Hosted within du's local data centres, this platform offers a secure, compliant, and scalable cloud environment that supports the needs of public sector entities, regulated industries, and strategic national enterprises by providing over 100 Oracle Cloud Infrastructure (OCI) services, enhanced by du's value-added offerings and localised operations.

Table of Contents

Executive Summary	02
Digital Sovereignty is a National Priority	04
The Evolving Regulatory Landscape in the UAE	04
The Rise of Sovereign Cloud	06
AI Adoption and Sovereign Clouds	07
Understanding Sovereign Clouds	08
Sovereign Cloud Deployment Models	08
Adopting Sovereign Cloud: Best Practices	09
What to Look for in Sovereign Cloud Solutions	09
Addressing the Challenges with Sovereign Cloud Deployments	10
Choosing a Sovereign Cloud Provider	11
du Sovereign Cloud Built on Oracle Alloy	13
Accelerating Sovereign AI	13
Key Features of du Sovereign Cloud Built on Oracle Alloy	13
Cloud Solution Portfolio	15
Adherence to Key Pillars of Digital Sovereignty	17
Conclusion and Essential Guidance	18

Digital Sovereignty is a National Priority

In today's interconnected landscape, digital sovereignty has become a strategic imperative for both nations and organisations. It refers to managing and controlling digital infrastructure, data, and technologies without external dependency or interference, spanning domains like data privacy, national security, political autonomy, and economic self-sufficiency.

Digital sovereignty empowers countries to enforce their own data protection laws, ensuring that sensitive information, such as citizens' healthcare records, is processed in alignment with national standards. It also plays a crucial role in national security by mitigating cyberattacks, espionage, and digital warfare risks by managing critical systems within national borders.

Sovereignty over digital ecosystems is also vital for maintaining political and economic independence. By governing their own digital ecosystems, countries can protect institutions from foreign influence and manipulation. Moreover, by fostering local technology ecosystems, nations can drive innovation, create high-value jobs, and retain more economic value locally. Sovereign digital infrastructure thus becomes more than a compliance tool, but a catalyst for economic resilience and global competitiveness.

The Evolving Regulatory Landscape in the UAE

The United Arab Emirates (UAE) has rapidly positioned itself as a global technology hub, attracting investors, entrepreneurs, and innovators from around the world. This transformation has been fuelled by proactive government strategies, significant digital infrastructure investments, and a clear national vision to diversify the economy beyond oil. Today, 77% of mid-sized and large enterprises in the UAE consider themselves digital businesses, having adopted a digital-first approach and scaled technology deployments across their operations.

As the UAE's digital maturity increases, digital sovereignty has become a central policy focus. The country has implemented several forward-thinking regulations and initiatives to safeguard its citizens' privacy, digital infrastructure, and data assets. For businesses operating in the UAE, understanding and complying with this evolving regulatory landscape is crucial.



Table 1: Key Policies and Regulations Driving Digital Sovereignty in the UAE

Name	Description
Smart Data Framework	Provides guidelines for data classification, localisation, and sharing across government entities, reinforcing state control over public-sector data.
Personal Data Protection Law (PDPL)	Establishes an independent data protection regime, restricting unauthorised cross-border data flows and strengthening local data governance.
National Cybersecurity Strategy	Enhances national cyber resilience through localised risk management practices and coordinated threat response capabilities.
National Cloud Security Policy	Sets standards for secure cloud adoption, emphasising in-country data residency and the use of accredited cloud providers.
DESC Information Security Regulation	Sets standards for Dubai Government Entities to ensure continuity of critical business processes and minimise information security-related risks and incidents.
UAE Information Assurance (IA) Regulation	Provides management and technical information security controls for entities to establish, implement, maintain, and continuously improve information assurance.
CBUAE Regulations	A set of regulations and standards by the Central Bank of the UAE that require financial institutions to enforce stringent data controls and host critical infrastructure in sovereign environments within the UAE.
ADGM Guidelines	A set of regulations and guidelines by Abu Dhabi Global Market that encourage financial firms to process personal and financial data locally and choose cloud providers that meet ADGM’s security and audit standards.
DIFC Laws and Guidelines	A set of laws and guidelines by Dubai International Financial Centre that emphasise local accountability in cross-border data handling and promote compliance with sovereignty-focused IT infrastructure assessments.
UAE Healthcare Data Law	Prohibits overseas storage of health data without explicit approval, ensuring such data is hosted within UAE-licensed entities.

Source: IDC, 2025

These initiatives reflect the UAE’s intent to not only become a digital innovation leader but also a trusted custodian of its digital future. By embedding sovereignty requirements into sector-specific regulations, the government is laying the groundwork for secure and compliant digital transformation across industries.

¹ Source: IDC Digital Executive Sentiment Survey 2024 (UAE, N=100, 250+ employees).

The Rise of Sovereign Cloud

Over the past two decades, cloud computing has become a cornerstone of digital transformation, enabling organisations across industries to scale operations, foster innovation, and respond to changing business demands. Cloud is no longer viewed as a mere infrastructure upgrade it is now a strategic enabler that aligns IT capabilities with core business goals.

As enterprises transitioned from traditional on-premises environments to hybrid and multi-cloud architectures, they encountered a key challenge: loss of control over critical data and workloads. This concern has been particularly pronounced in highly regulated sectors such as government, financial services, healthcare, and energy, where strict compliance and data governance are non-negotiable.

In response, sovereign cloud solutions have emerged as a vital solution. These offerings provide a secure, regulation-compliant environment by ensuring that data is processed, stored, and managed entirely within national borders, under the jurisdiction of trusted local entities.

Today, sovereign cloud is increasingly viewed as an integral part of the hybrid multi-cloud landscape that defines the modern enterprise IT environment. Its adoption is being driven by the dual imperatives of evolving regulatory requirements and the growing demand for transparency and trust in how data is handled.

Figure 1: Drivers of Sovereign Cloud Adoption in the UAE



Q. What are the main drivers behind your organization’s decision to use sovereign cloud?

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



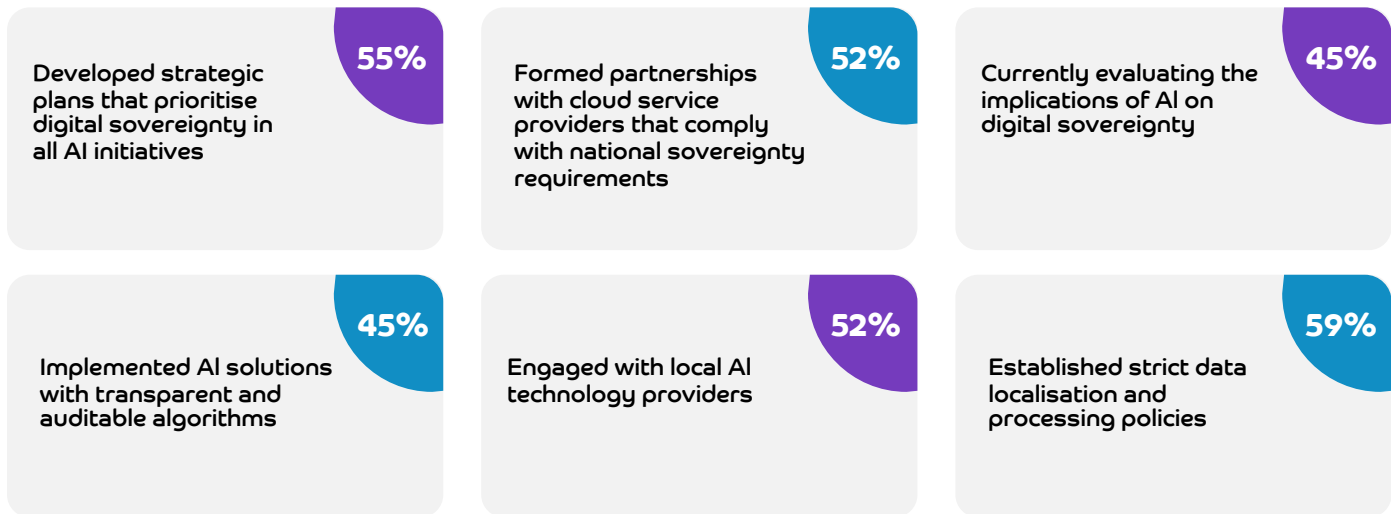
AI Adoption and Sovereign Clouds

Artificial Intelligence (AI) is fast becoming a strategic pillar of national innovation agendas. As AI adoption accelerates, governments and enterprises alike are embedding sovereignty considerations into their AI strategies to ensure compliance, autonomy, and responsible innovation.

In the UAE, 62% of organisations report that data sovereignty and access to sovereign cloud infrastructure influence their partner choices for AI projects. To support these ambitions, many are proactively integrating sovereignty principles into their AI development and deployment practices.

As AI systems become more deeply embedded into mission-critical functions, ranging from healthcare diagnostics to financial decision-making, organisations are demanding greater transparency, auditability, and control over how these systems are trained and operated. Sovereign cloud platforms play a pivotal role in fulfilling these requirements by offering localised infrastructure for training and inference, robust encryption mechanisms, and verifiable access controls. This ensures not only regulatory compliance but also builds trust among stakeholders by minimising the risk of data misuse or foreign interference.

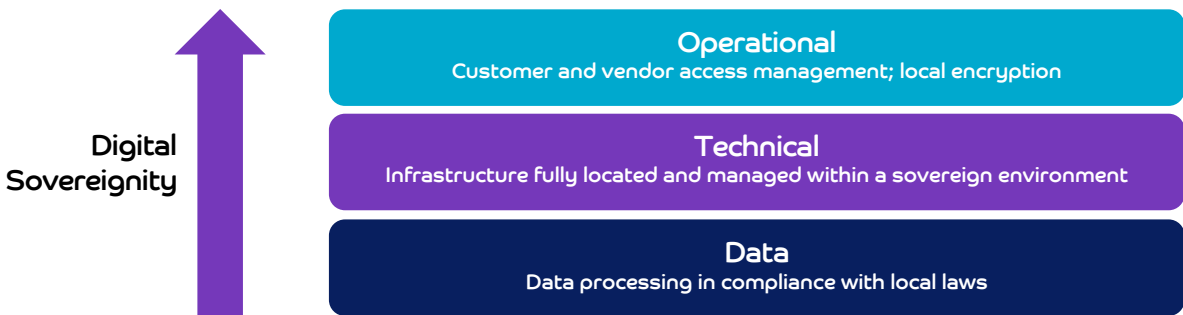
Figure 2: Steps Taken by UAE Organizations to Align AI with Sovereignty Principles



Q. What steps has your company taken to ensure AI technologies adhere to digital sovereignty principles?

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

Figure 3: Sovereign Cloud Deployment Models



Source: IDC Worldwide Sovereign Cloud Taxonomy, 2024

² Source: IDC Digital Sovereignty Survey June 2024 (N=30, UAE, 500+ employees).

³ Source: IDC Worldwide Sovereign Cloud Taxonomy, 2024

Understanding Sovereign Clouds

As the relevance of sovereign cloud continues to grow, it is critical for organisations to develop a deeper understanding of what it entails. Sovereign cloud is a specialised segment within the broader digital sovereignty domain, and it addresses the need for localised control over data, infrastructure, and operational governance.

According to IDC, digital sovereignty is defined as the capacity for digital self-determination by nations, organisations, and individuals. At its core, it gives data owners complete authority over where and how their data is stored, processed, and accessed down to the infrastructure layer and operational oversight.

The three key pillars of digital sovereignty include:

Data Sovereignty



Ensures that data is collected, classified, stored, and processed in compliance with local laws. This requires ongoing monitoring and adaptation to changing regulations and privacy standards

Technical Sovereignty



Involves the use of digital infrastructure, such as data centres, servers, and software, that is fully located and managed within a sovereign environment. This infrastructure must be insulated from foreign access and extraterritorial jurisdiction

Operational Sovereignty



Enables transparent control over operations, including service provisioning, access management, and infrastructure monitoring, ensuring that administrative authority resides within national borders.

Sovereign Cloud Deployment Models

Cloud is the foundation of digital business innovation, and by extension, a central element in the sovereignty conversation. Sovereign cloud is defined by who provides the cloud service, who owns and controls the infrastructure, where it is hosted, and who has access.

Both public and private cloud models can operate in sovereign configurations. Over time, various deployment approaches have evolved, offered either directly by hyperscalers, through local providers, or via partnerships between the two.

The two dominant deployment models are:

Public Cloud with Sovereign Controls

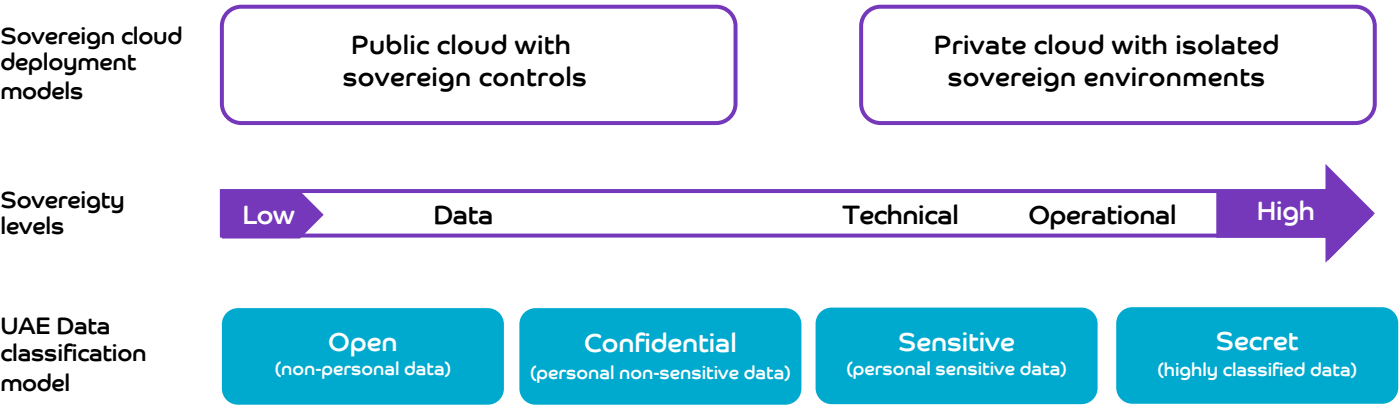
This model adds sovereignty features to a standard public cloud platform. Data residency is ensured by hosting in-country, while logical separation is achieved through tools like encryption key management and access control. This sovereign cloud model has two versions, depending on who manages the sovereign controls. In one version, the customer manages sovereignty controls. In another, a local partner independently manages the controls, ensuring strict local oversight. This model is best suited for open and confidential (non-sensitive) datasets as defined by the UAE Smart Data Framework.⁴

Private Cloud with Isolated Sovereign Environments

Here, a fully dedicated (private) cloud is delivered from sovereign data centres. This model achieves technical sovereignty through physical and logical isolation with dedicated hardware based on local cloud environments. To achieve higher levels of sovereignty and include operational aspects, local providers are partnering with Hyperscalers to create sovereign cloud solutions that cater to the highly regulated sectors and sensitive and secret datasets. The infrastructure is based on hyperscaler technology but fully controlled by a local provider, ensuring both innovation and sovereignty.

⁴ <https://u.ae/en/about-the-uae/digital-uae/data/data-operability>

Figure 4: Sovereign Cloud Deployment Models



Source: IDC Worldwide Sovereign Cloud Taxonomy, 2024

Adopting Sovereign Cloud: Best Practices

In today’s compliance-focused and innovation-driven environment, integrating sovereign cloud into an enterprise’s IT strategy is no longer optional, it is essential. However, navigating the evolving sovereign cloud landscape can be complex, and many organisations face challenges in identifying the right approach.

This section outlines key best practices to ensure successful sovereign cloud adoption, focusing on what to look for in providers, how to address common barriers, and how to align solutions with business and regulatory priorities.

What to Look for in Sovereign Cloud Solutions

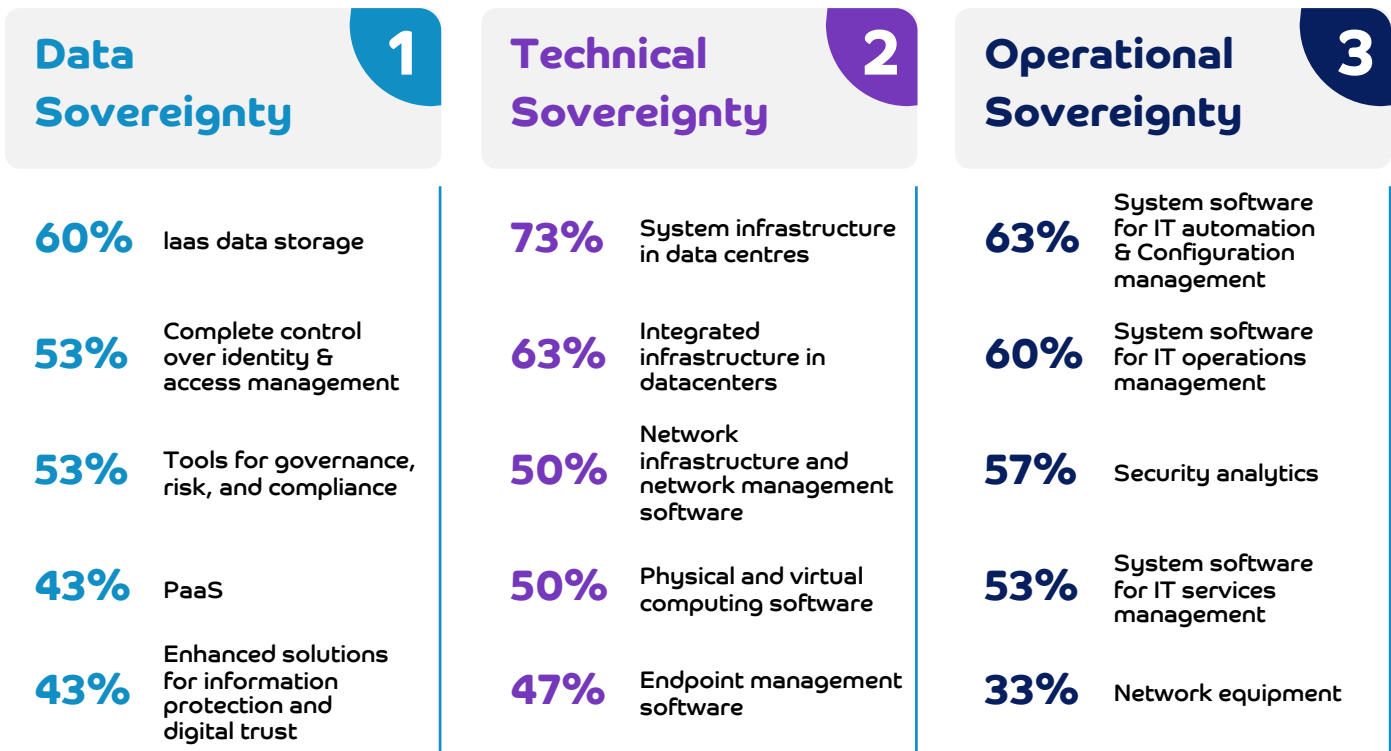
As outlined earlier, sovereign cloud encompasses three critical domains: data sovereignty, technical sovereignty, and operational sovereignty. Each organisation will have unique requirements depending on its industry, jurisdiction, and regulatory obligations.

The primary driver for sovereign cloud adoption is the need to meet regulatory and legal compliance, especially in highly regulated sectors. This typically requires foundational Infrastructure-as-a-Service (IaaS) components for secure data storage and protection, as well as Platform-as-a-Service (PaaS) solutions tailored to national standards.

Data classification plays a vital role in this process. By evaluating the sensitivity of datasets, organisations can determine which workloads must be migrated to sovereign environments. Importantly, sovereignty does not end with data at rest. Ensuring security for data in motion, especially across networks, is equally important, and this involves applying controls to a complex mix of technologies and cross-border pathways.



Figure 5: IT Solutions Needed for Data, Technical, and Operational Sovereignty



Q. What IT solutions does your organisation need for data sovereignty, technical sovereignty, and operational sovereignty as part of its sovereign cloud?

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

Addressing the Challenges with Sovereign Cloud Deployments

While sovereign cloud adoption is strategically important, the journey is often complex and requires proactive planning. Organisations must address both technical and operational challenges to successfully implement and scale sovereign cloud environments.

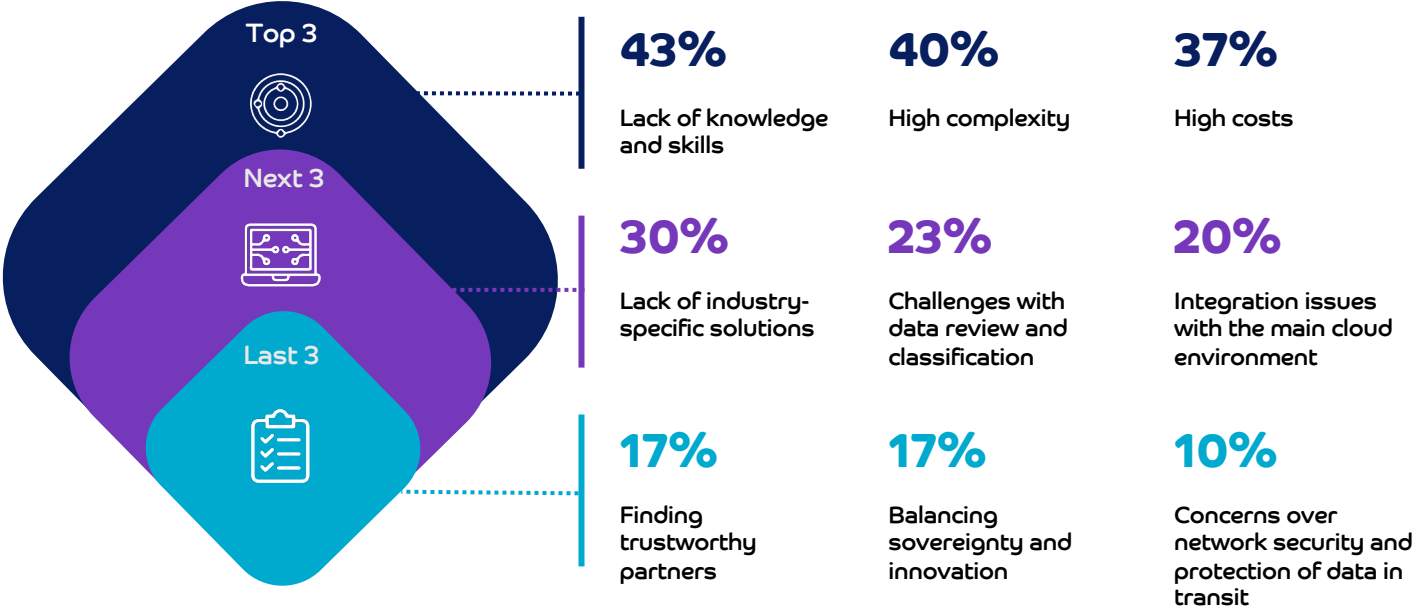
The first step is a comprehensive assessment of sovereignty requirements. This includes:



Skill shortages are a common challenge. Most organisations lack in-house expertise to manage sovereign cloud environments. This can result in added costs for training or recruitment, — particularly for roles that require specialisation in data governance, cybersecurity, cloud operations, and even legal knowledge related to jurisdictional compliance. Additionally, aligning internal governance with external regulatory frameworks requires strong cross-functional collaboration between IT, legal, compliance, and business units.



Figure 6: Challenges with Sovereign Cloud Deployments



Q. What are your organisation's main challenges in implementing sovereign cloud?
Source: IDC Digital Sovereignty Survey June 2024 (N=30, UAE, 500+ employees)

Choosing a Sovereign Cloud Provider

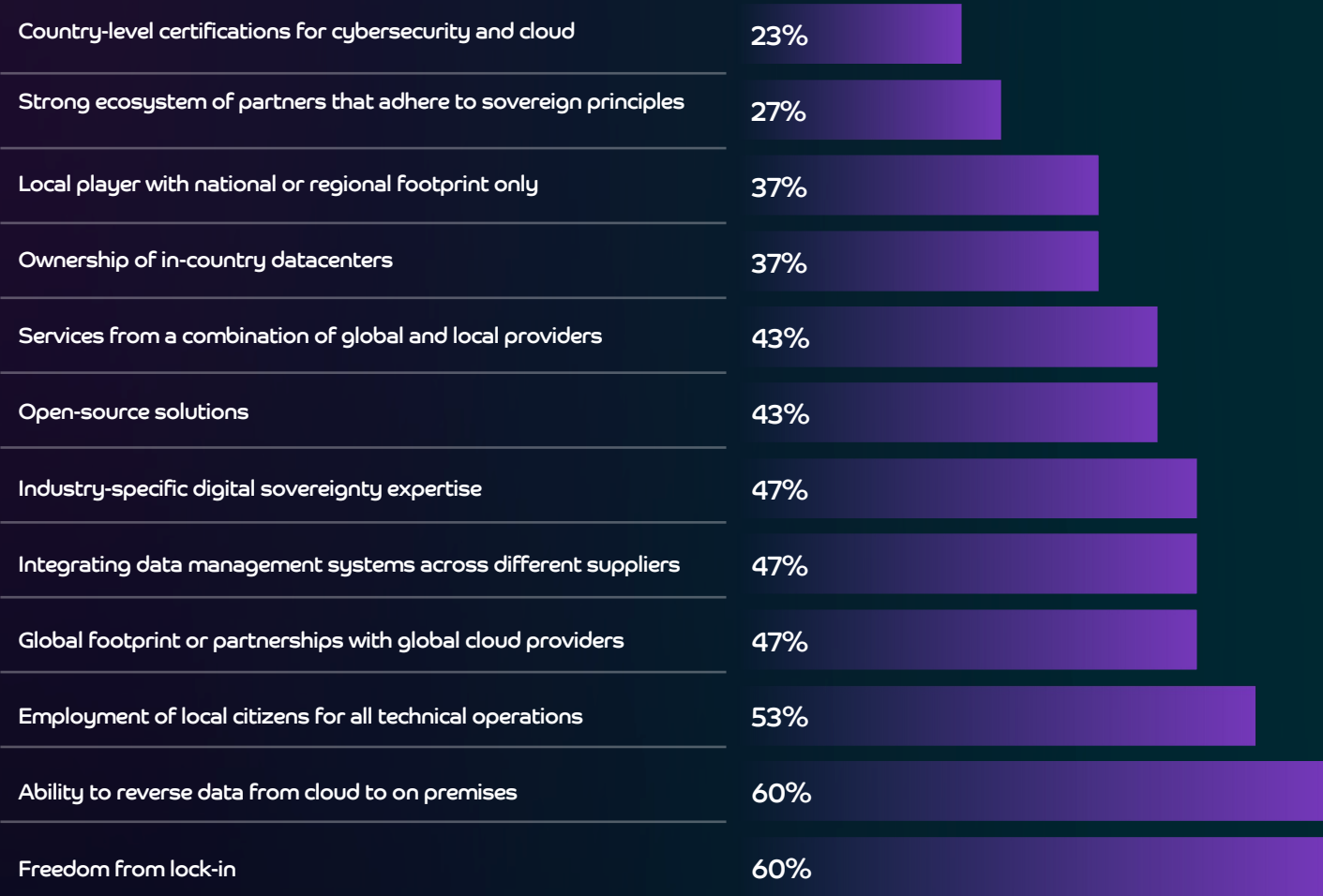
Selecting the right partner is critical to the success of any sovereign cloud strategy. The provider must not only deliver compliant technology but also act as a strategic advisor who can guide organisations through policy interpretation, risk mitigation, and solution design.

Trust is foundational. It extends beyond the core vendor to include their entire ecosystem of partners, support teams, and service providers. Transparency, local accountability, and proven expertise in regulatory environments are essential attributes to evaluate.

Organisations should look for an ecosystem-based approach, combining global hyperscalers' scale and innovation with the local expertise, governance, and operational control provided by national partners. This also applies to global SaaS vendors that need to operate within sovereign frameworks while meeting enterprise workload demands.



Figure 7: Key Attributes to Evaluate Sovereign Cloud Providers



Q. Which attributes are important when choosing a sovereign cloud partner or provider?
Source: IDC Digital Sovereignty Survey June 2024 (N=30, UAE, 500+ employees)

du Sovereign Cloud

Built on Oracle Alloy

du is UAE's leading telecom and technology provider with a comprehensive portfolio of mobile, fixed, broadband, entertainment services, and fintech solutions. Through a digital-first approach powered by fibre and 5G technology, du delivers solutions leveraging cloud computing, AI-driven analytics, advanced cybersecurity, and IoT integration. As a digital telco enabler spearheading the UAE's digital transformation, du collaborates with a dynamic partner ecosystem to propel industries and society toward operational excellence, shaping a more connected and digitally advanced future across the region.

To meet the rising demand for sovereign digital infrastructure in the UAE, du has partnered with global hyperscaler Oracle to launch a sovereign cloud solution tailored specifically for the UAE market.

Through this collaboration, du will deploy Oracle Alloy, a cloud infrastructure platform that enables partners to operate and customise Oracle Cloud Infrastructure (OCI) services independently. The solution will be hosted in du's local data centres, ensuring that data remains within UAE jurisdiction and under national legal and administrative control.

The result is a sovereign, in-country cloud region that delivers both hyperscale capabilities and regulatory compliance. This platform is designed to serve UAE public sector entities, strategic industries, and large enterprises seeking full sovereignty over their cloud operations.

Using Oracle Alloy, du will offer access to over 100 OCI services, including compute, storage, database, and AI services, augmented by du's own managed cloud services and applications. These services will be customised for the UAE market, ensuring alignment with local regulatory frameworks, industry-specific needs, and Arabic language support.

Accelerating Sovereign AI

The partnership will also benefit from Oracle's collaboration with NVIDIA, bringing cutting-edge GPU acceleration and AI capabilities into the sovereign cloud platform. du will introduce GPU-as-a-Service, enabling customers to run sovereign AI workloads, including generative AI models, within a fully compliant environment.

Oracle's distributed cloud architecture, combined with NVIDIA's AI and accelerated computing stack, will allow du to deliver high-performance, sovereign AI solutions that meet data localisation, governance, and privacy mandates.

Key Features of du Sovereign Cloud Built on Oracle Alloy

The du Sovereign Cloud solution has been designed specifically to meet the elevated requirements of sovereign and regulated workloads in the UAE. The platform integrates Oracle's robust cloud technologies with du's localised operations, offering organisations both technical excellence and regulatory alignment.

Below are the key features that distinguish this sovereign cloud solution:



Sovereign Community Cloud

The cloud region operates as a dedicated sovereign community cloud, hosted entirely within the UAE and managed under the legal authority of local entities. Access to the platform is controlled by du, ensuring that only government entities, semi-government organisations, and strategic national enterprises are eligible. This sovereign-by-design architecture supports national mandates on data residency, access control, and jurisdictional compliance.



Tenant-Isolated Services

To protect highly sensitive workloads, the solution offers complete logical, operational, and when needed, physical isolation between tenants. Customers can deploy Dedicated Virtual Machine Hosts, Bare Metal Servers, Shielded Instances, and Confidential Compute. These technologies ensure hardware-level isolation, full control over hypervisors, and protection from firmware-level threats.



Zero Trust Security Architecture

The platform is built on a Zero Trust model, where no user, system, or device is implicitly trusted. Every access request is authenticated, authorised, and continuously validated. Defence-in-depth controls span identity, network, compute, and data layers, reducing attack surfaces and enhancing threat response.



Secure Landing Zones

The solution comes with CIS/DESC-compliant landing zones, pre-configured using infrastructure-as-code to enforce policy-based controls from day one. These landing zones support secure networking, central logging, and identity segmentation aligned with Zero Trust principles.



Dedicated Network Connectivity

All network pathways are physically isolated and locally controlled. du manages private connections between customers and Oracle operations. Public internet exposure is minimised, ensuring high data-in-transit security and reduced external risk.



Bring Your Own Encryption (BYOK) and HSM Support

Customers maintain full control over encryption and cryptographic keys. The system integrates with external Key Management Systems (KMS) and supports customer-owned Hardware Security Modules (HSMs). Neither du nor Oracle can access customer keys, even during operations, enabling complete cryptographic sovereignty.



Locally Vetted, Arabic-Speaking First Line Support

Support is fully operated within the UAE by vetted personnel who meet national security clearance criteria. Arabic-speaking first-line agents ensure rapid response and cultural alignment ensuring trust and contextual relevance.

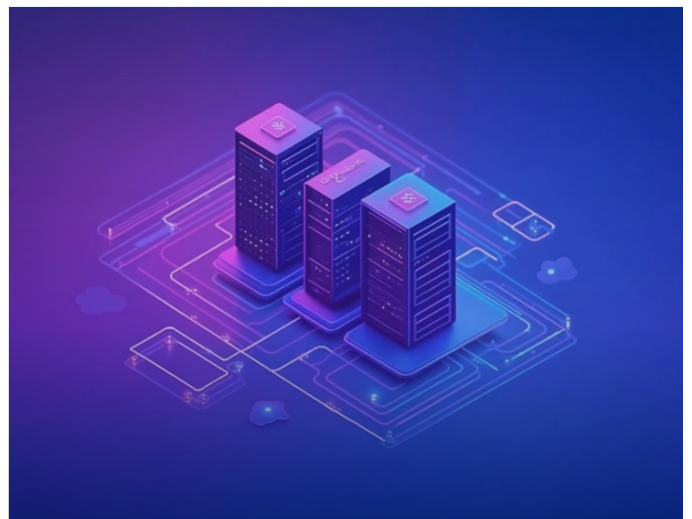









Figure 8: Key Features of du Sovereign Cloud Built on Oracle Alloy

Sovereign Community Cloud 	Tenant-Isolated Services 	Zero Trust Security Architecture 	Secure Landing Zones 
Dedicated Network Connectivity 	Bring Your Own Encryption (BYOK) and HSM Support 	Locally Vetted, Arabic-Speaking First Line Support 	

Source: du and Oracle, 2025

Cloud Solution Portfolio

The du Sovereign Cloud built on Oracle Alloy offers the full breadth of Oracle Cloud Infrastructure (OCI) services in a secure, sovereign environment. Customers benefit from the scalability and flexibility of public cloud, while retaining full control over data residency, compliance, and security.


This enables UAE-based organisations to innovate confidently, meet evolving regulatory obligations, and support demanding workloads, including AI, analytics, and enterprise applications. Customers can start small and scale seamlessly, accessing a comprehensive set of cloud services across infrastructure, platform, and software layers:

Core Infrastructure

Includes foundational services to support a wide range of workloads:


Compute

Virtual machines, bare metal servers, GPU instances, and container services.




Storage

Block, object, and file storage options.




Networking

Virtual cloud networks, private connectivity, and load balancers.



Kubernetes and orchestration

OCI Container Engine and integrated tools for scalable containerised apps.



Data Management

Offers advanced capabilities for storing, analysing, and managing data:

Oracle **Database** and MySQL services, with high availability and performance tuning.

Data Science and AI tools, including model training, deployment, and monitoring

Analytics and visualisation tools for insights-driven decision-making.

Developer Services

Empowers development teams to build, integrate, and automate faster:

API Management for secure and scalable integrations.

Oracle APEX for **low-code application** development.

Functions, Queues, Events, and Workflows to **support serverless computing** and event-driven architectures.

Governance and Administration

Provides centralized control and visibility across services:

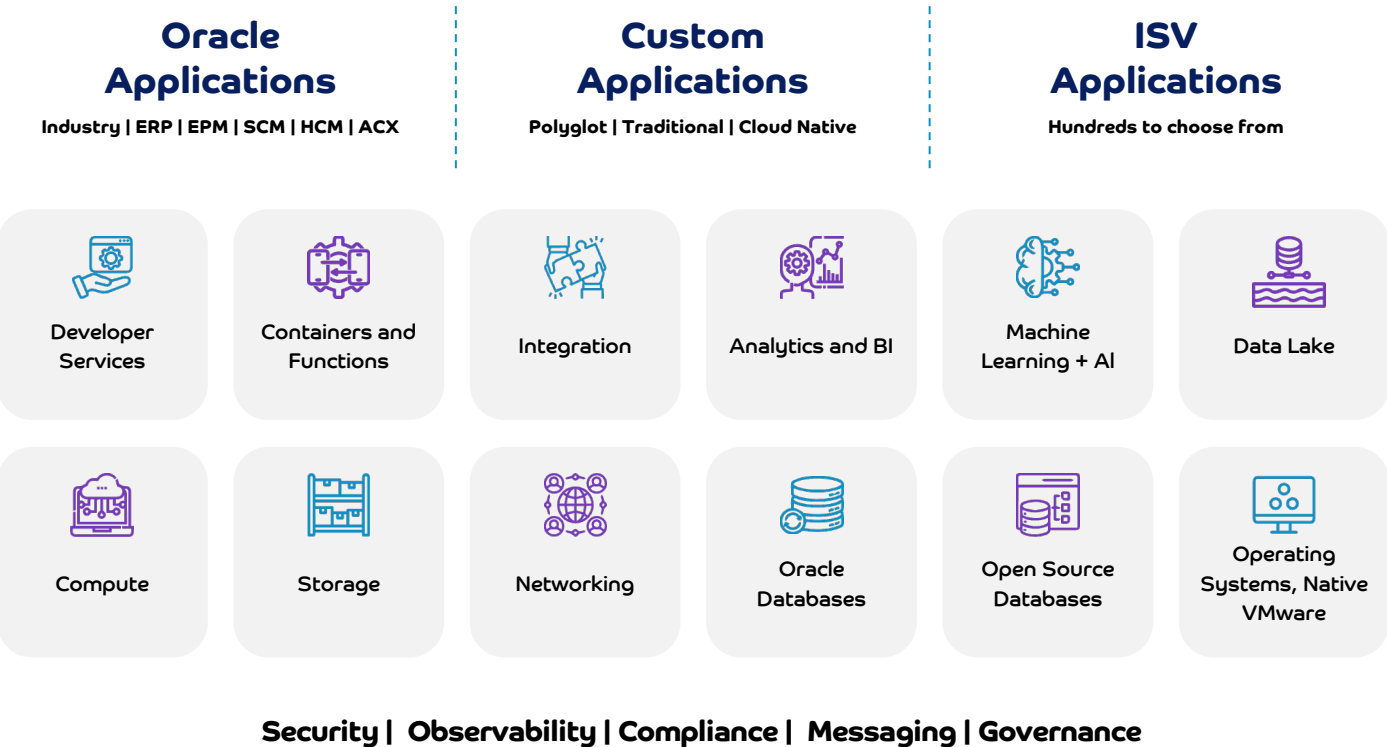
Identity and Access Management (IAM) with fine-grained policies.

Security tools including key management, vulnerability scanning, and compliance dashboards.

Observability and Management services for end-to-end visibility into application and infrastructure performance.



Figure 9: Portfolio of Cloud Solutions in du Sovereign Cloud Built on Oracle Alloy



Source: du and Oracle, 2025

Adherence to Key Pillars of Digital Sovereignty

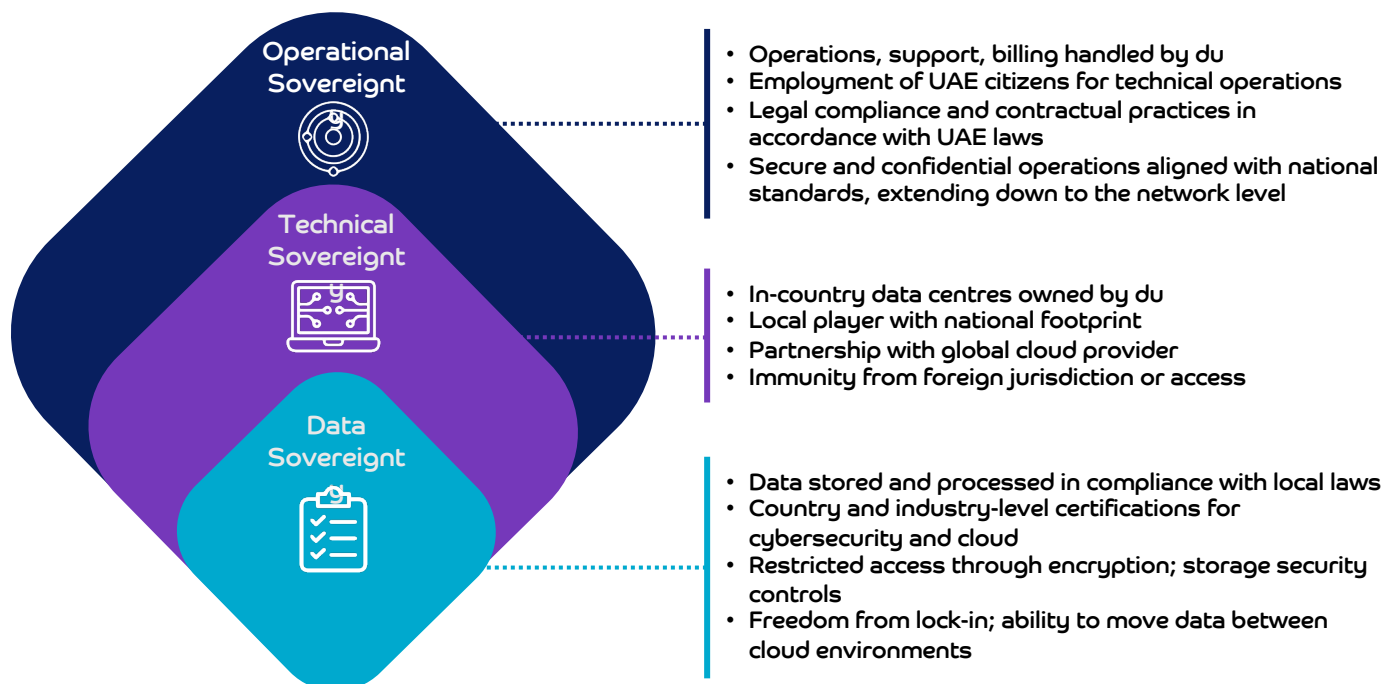
The du Sovereign Cloud Built on Oracle Alloy aligns with the three core pillars of digital sovereignty and reflects the key attributes that end-user organisations seek in a sovereign cloud provider, as outlined earlier in this whitepaper. This joint solution combines Oracle's global technology leadership with du's deep regional expertise, delivering a unique offering that merges global innovation with strict local compliance.

The presence of in-country data centres ensures both data and technical sovereignty by adhering to national and industry-specific regulations governing data processing, cybersecurity, and digital infrastructure. du's network infrastructure further reinforces these controls, extending security measures down to the network level.

Operational sovereignty is achieved through locally managed operations, support, and billing, fully compliant with UAE legal and contractual standards. The inclusion of local talent in service delivery not only ensures regulatory alignment but also fosters in-country value creation and skills development. Additionally, du's hybrid multi-cloud capabilities and managed IT services enable seamless data mobility across environments, minimizing the risk of vendor lock-in and enhancing overall cloud agility.



Figure 10: How the du Sovereign Cloud Built on Oracle Alloy Enables Digital Sovereignty



Source: du and Oracle, 2025

Conclusion and Essential Guidance

Organisations across sectors are facing growing regulatory complexity, heightened cybersecurity risks, and rising expectations around responsible data stewardship. Against this backdrop, sovereign cloud has emerged as a critical enabler of digital resilience, national security, and innovation. It provides the control, transparency, and assurance organisations need to operate securely and confidently in an increasingly interconnected and compliance-driven world.

To successfully navigate the shift toward sovereign cloud, organisations must adopt a deliberate strategy. This begins with assessing data classification requirements, mapping workloads to appropriate deployment models, and building internal governance aligned with national frameworks. Equally important is choosing the right partner, one that brings global capabilities, local presence, and the regulatory fluency required to manage complex jurisdictional needs. Without the right guidance and ecosystem, even the most advanced cloud architecture can fall short on sovereignty goals.

Essential Guidance for Tech Buyers:

Embed Sovereignty into Strategy



Treat digital sovereignty as a core element of your IT, risk, and data governance strategy. It must be factored into procurement, architecture, and operations, not treated as an afterthought.

Prioritise Compliance and Control



Focus on platforms that provide end-to-end visibility, data localisation, and auditable security controls. Pay close attention to network security and operational oversight, not just data at rest.

Build Local Alliances



Partner with providers who have a proven regional footprint and strong ties to local regulatory bodies. These alliances are key to ensuring continuity, cultural alignment, and trust.

Think Long-Term



Sovereign cloud is not just about meeting today's compliance, it is about building a scalable, future-ready foundation for AI, multi-cloud, and digital innovation under national control.

By taking a proactive, sovereignty-first approach, UAE organisations can position themselves as both regional leaders in compliance and global frontrunners in trusted digital innovation.



About du

du adds life to life with a comprehensive portfolio of mobile, fixed, broadband, entertainment services, and fintech solutions. Through a digital-first approach powered by ultra-reliable fiber and 5G technology, du delivers bespoke solutions leveraging cloud computing, AI-driven analytics, advanced cybersecurity, and IoT integration. As a trusted digital telco enabler spearheading the UAE's digital transformation, we collaborate with a dynamic partner ecosystem to propel industries and society toward operational excellence, shaping a more connected and digitally advanced future across the region.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

 IDC Middle East/Africa
Level 15, Thuraya Tower 1 - Dubai Media City
Dubai, United Arab Emirates - P.O. Box 500615

 +971.4.3912741
 @IDC | idc-community.com | www.idc.com

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2025 IDC. Reproduction without written permission is completely forbidden.