November 2026
InfoBrief
Sponsored by Cohesity

Digital Sovereignty:

A Guide for Managed Service Providers





Rahiel Nasir
Research Director and Lead Analyst,
Digital Sovereignty, IDC



David Tapper
Program Vice President,
Outsourcing and Managed Cloud Services, IDC

Table of contents

Click any title to navigate directly to that page.

Executive summary:
Meeting digital sovereignty demands in a changing landscape 3

Rethinking infrastructure for digital sovereignty 4

The role of managed service providers 5

The digital sovereignty stack 7

Baseline definition: The digital sovereignty stack 8

Why digital sovereignty? 9

Scoping and positioning sovereign services 10

Choosing a sovereign cloud deployment model 11

Deciding the market you want to serve 12

Data protection and resilience: Key pillars for digital sovereignty 13

IDC's digital sovereignty stack 14

Pain points: The differentiation opportunity 15

What sovereign cloud customers are looking for 16

Aligning to regional rules: The EU's SEAL ratings 17

Essential guidance 18

About the IDC analysts 19

Message from the sponsor 20

Executive summary:

Meeting digital sovereignty demands in a changing landscape

Today's buyers are confronted with a complex landscape of rapidly changing technologies and business needs that are placing major challenges in their ability to optimize operations and financial success. Digital sovereignty has become one of these needs for which organizations are seeking support from managed service providers (MSPs) that must meet the sovereignty requirements on the next page.



Rethinking infrastructure for digital sovereignty

Delivering the right value

- **Resiliency**
  Incorporating critical capabilities such as robust security and recoverability, mitigating concentration risk of suppliers, and utilizing management platforms and control planes to optimize performance
- **Quality of service**
  Meeting service-level agreements (SLAs) and service-level objectives (SLOs) that include tiered commitments of performance, sovereignty (such as data residency, control, and much more), and support for AI involving output quality, performance, and agent behavior
- **Industry expectations**
  Supporting regulatory requirements and sector rules including certifications and standards along with meeting contracting terms such as authorized personnel, flow-down, data ownership, and access rights
- **Geopolitical policies**
  Enforcing policy and legal requirements of jurisdictional boundaries spanning legal, regulatory, and enterprise involving extraterritorial laws, export controls and sanctions, and trade and localization standards

Demonstrating expertise

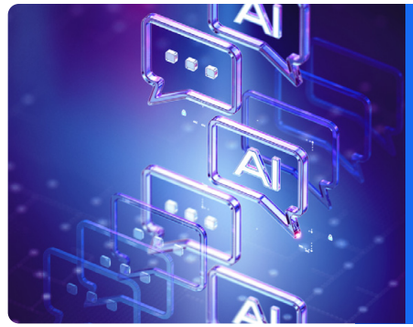
- **Knowledge**
  Having in-depth knowledge of critical building blocks for a digital sovereignty stack such as strategic assurance and governance as well as business and IT assurance
- **Best practices and competencies**
  Providing offerings that assist in meeting sovereignty needs such as aligning workloads by deployment model, provisioning technology innovation and business capabilities including cost and economic management, and managing legal and geopolitical risks
- **Complexity**
  Supporting complex sovereignty requirements that include selecting the right deployment model, enforcing an array of regulatory factors, managing technological complexity that increasingly involves AI and the need for data hygiene, and optimizing partnership ecosystems including supply chain
- **Performance**
  Meeting an expanding set of operational requirements such as continuous compliance and assurance, resilience and incident response, adapting to policy changes, and ensuring continuous improvement and skills development

The role of managed service providers

Expectations of MSPs in supporting client need for digital sovereignty extensive capabilities.

Buyers looking to MSPs to support their sovereign requirements have the following broad set of expectations that these providers must fulfill:

- **Business processes**
  Understand the extent to which business processes are bounded by regulatory and compliance requirements as well as operate across jurisdictions, particularly international
- **Resiliency**
  Incorporate robust security, business continuity/disaster recovery, use of hybrid clouds and edge computing, and multicloud operations which can deploy the same IP and data across multiple public cloud providers, all within the client's sovereign boundary
- **Repatriation**
  Repatriate IP and data hosted on a public cloud back to a private cloud due to poor performance of the public cloud, security issues, external events (e.g., climate impacts, changes in international trade, geopolitical conflicts), and compliance factors
- **Quality of service**
  Support meeting critical SLOs and SLAs such as performance and latency, availability, time to resolution, recovery point objectives (RPOs), and recovery time objectives (RTOs)
- **Industry requirements**
  Not only understand industry regulations across multiple jurisdictions but also adapt to changes in regulations more rapidly

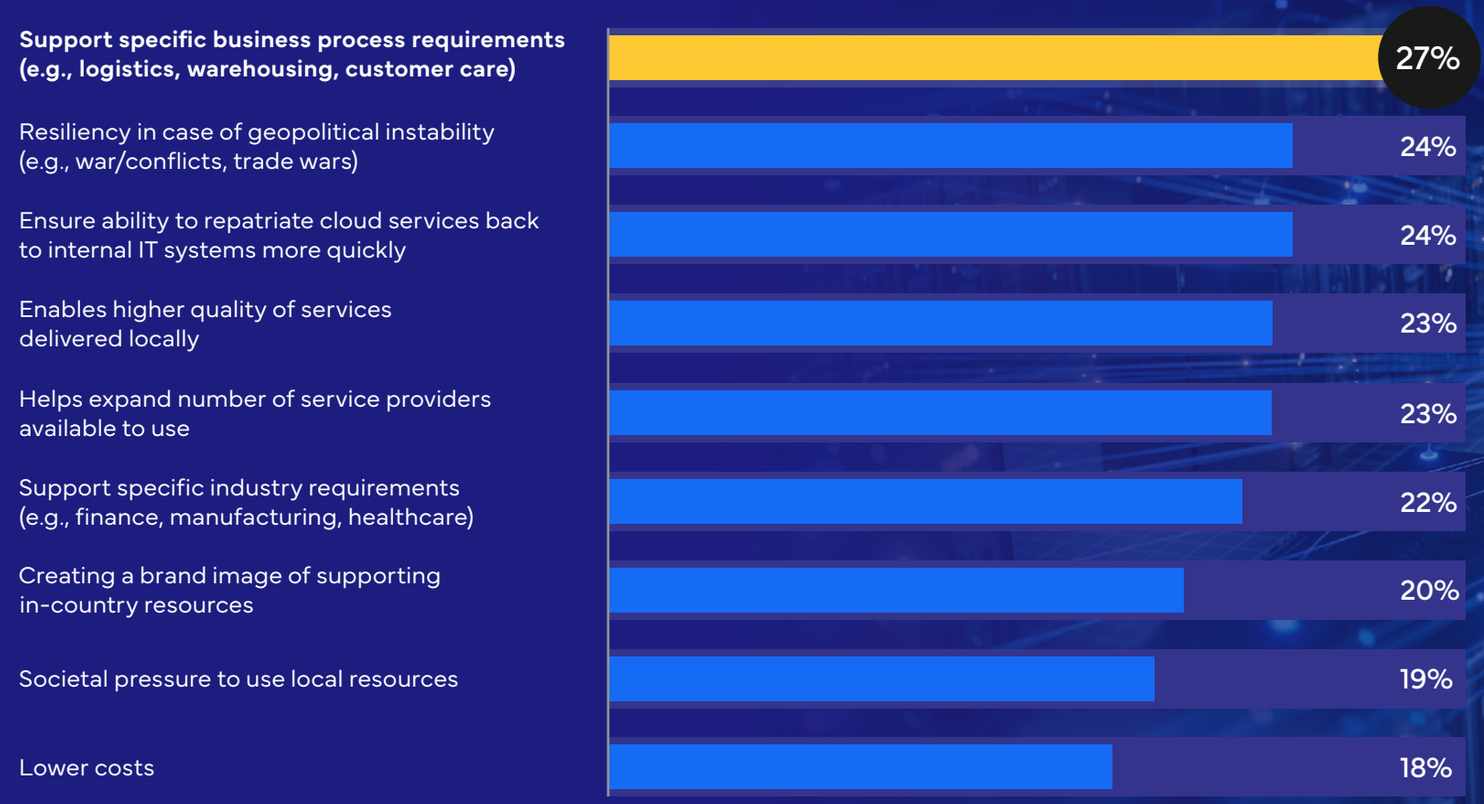


With the incorporation of AI as part of managed services, organizations will expect their MSPs to have developed the appropriate AI risk management capabilities across key areas involving security, privacy, and compliance, which would include compliance for sovereign clouds.

The role of managed service providers (continued)

Primary drivers for using managed cloud services for sovereign clouds

(Share of respondents worldwide)



n = 1,514; Source: IDC's *Worldwide Managed Cloud View Survey*, 2024

The digital sovereignty stack

Unpacking the "sovereign cloud" headline label into specific layers and dimensions, with clear roles and responsibilities across stakeholders including MSPs.

IDC formally defines digital sovereignty as
"the capacity for digital self-determination by nations, organizations, and individuals."

- Digital sovereignty means giving data owners total control and choice over how and where their data is managed, stored, and processed by service providers.
- This includes all underlying infrastructure used for the data, such as datacenters and networks, as well as the support and admin staff who have access to that data and infrastructure.
- Digital sovereignty is about more than just data localization. It covers data, technical, operational, assurance, supply chain, and geopolitical dimensions.
- Data sovereignty and sovereign cloud can be considered as subsets of digital sovereignty. AI sovereignty has emerged as a new frontier.
- There are many aspects to digital sovereignty as depicted by the IDC "Digital Sovereignty Stack."

Source: IDC's *Worldwide Digital Sovereignty Taxonomy*, 2026

Baseline definition: The digital sovereignty stack

Deployment strategy and operating model

Strategic assurance (geopolitical)
Self-sufficiency, trading partnerships, regulations, tariffs

Governance assurance (risk management)
Governance, compliance, data security, service quality and objectives, business resiliency

Business assurance (operations)
Support and admin, service levels, controls, authentication, authorization, auditing business continuity and recovery

IT assurance (supply chain)
Procurement and manufacturing, raw materials, energy, workforce and labor, transportation

Infrastructure
Compute, storage, networking

Platforms
Business intelligence, decision support, AI, data management

Applications
AI native, cloud native, traditional

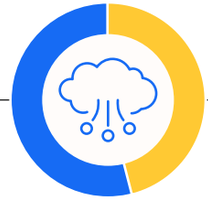
Data residency, security, and privacy

Source: IDC's *Worldwide Digital Sovereignty Taxonomy*, 2026

Why digital sovereignty?

Core value proposition of digital sovereignty is centered on data security, compliance, and operational resilience for which MSPs need to invest in capabilities that can help achieve these objectives.

Globally, **54%** of organizations currently use sovereign cloud solutions,



while **46%** plan to use them in 12 months or after.

- Digital sovereignty is of interest to all industries, not just those in regulated sectors.
- The need for greater operational and business resilience is one of the top market drivers. Resilience is a key tenet of digital sovereignty, and data protection and assurance are vital here, as recent conflicts have highlighted.
- Geopolitical tensions, economic uncertainties, and regulatory changes are also having an impact: 73% say that since the start of 2026, their interest in implementing digital sovereignty solutions has increased as a direct result.

51%
To increase data privacy and security

38%
Compliance with industry regulations/local laws

35%
To provide greater operational/business resilience

34%
To better manage IT vendor risk

31%
To increase customer trust

28%
Digital sovereignty is now part of the business strategy

25%
To protect against extraterritorial data requests

25%
Protection against geopolitical risks

20%
To expand internationally

n = 633; Source: IDC's *Worldwide Digital Sovereignty Survey*, June 2026

Scoping and positioning sovereign services

MSPs should scope and position their sovereign services around a road map that assesses which workloads must meet sovereign requirements and then identifies the right deployment model for each workload.

- Not all workloads and data need to be migrated to a sovereign cloud. MSPs should scope services around those subject to regulatory compliance and/or comprising data classified with high sensitivity ratings, rather than positioning sovereignty as a blanket offering.
- Almost half of all corporate data now sits in the top two sensitivity tiers. On average, organizations categorize 27% of their data as highly sensitive or restricted, and 21% as mission-critical or highly restricted.
- Customers will look to partners who can demonstrate sovereign expertise in their operational jurisdictions, so MSPs should position themselves as the guide for their clients' ongoing digital sovereignty journeys.

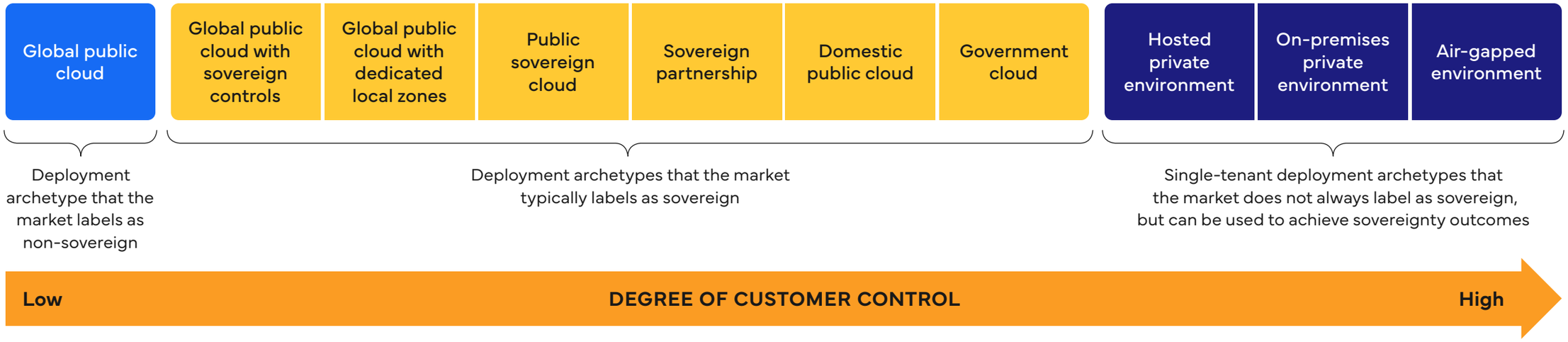
Steps for MSPs to scope services

Review	Security and compliance processes, tools, and skills
Classify	Data and apps by sovereignty requirements and workloads
Control	Apply sovereignty controls to those data and apps
Develop	Specific programs to enable you to execute on sovereignty
Balance	Sovereignty requirements with innovation needs
Maintain	Security and compliance processes on an ongoing basis

n = 625 (data classification), n = 621 (data storage); Source: IDC's *Worldwide Digital Sovereignty Survey,* June 2026

Choosing a sovereign cloud deployment model

Sovereignty is not a binary choice but spans use of multiple types of deployment models, each determined by different degrees of sovereign rules and policies for which MSPs must ensure optimal alignment of workloads by deployment models based on in-depth knowledge of sovereign requirements with access to required partnerships.



These 10 archetypes represent the deployment models that are currently available in the market. However, it is important to constantly monitor new offerings that technology suppliers are bringing to market at a rapid pace, because IDC expects new archetypes could emerge.

Deciding the market you want to serve

Complexities of sovereignty mandate MSPs to perform due diligence in aligning workloads by sovereign requirements while ensuring control and adaptability.

Ensuring control and adaptability, a means of mitigating risks, requires robust governance over data and IP including compliance engineering particularly with AI, service expertise including industry expertise, and critical capabilities such as control and management planes, cost and economics management, and security and recovery.

Workload-specific considerations

- How sensitive or regulated is the **data?** Does regulation designate the data as sensitive, confidential, or top secret, and mandate specific requirements on storage and processing?
- How sensitive or regulated is the **use case?** Is the use case designated as high-risk by regulation (e.g., the EU AI Act)?
- How strategically relevant is it to control the **IP** embedded in the system?
- How important is it to adopt leading-edge **innovation?**
- How much does the workload need to adapt to accommodate **large-scale** performance and future growth in users/usage?
- How important is it to be independent from the vendor in terms of **system architecture** design, interoperability, and portability?

Organizational considerations

- What is the organization's **mindset** with respect to sharing risks and controls with suppliers?
- What type of technical and business **competencies** has the organization invested in or is ready to invest in?
- How does the organization manage the **economics** of IT?
- How regulated is the **industry** in which the organization operates?

Market considerations

- What is the global **geopolitical** environment like?
- What kind of sovereign posture are **national policymakers** promoting?
- How are global **technology suppliers** evolving their offerings in response to the geopolitical environment and countries' sovereignty policies and postures?

Data protection and resilience: Key pillars for digital sovereignty

Sovereignty is not just about where data resides. It is also about resiliency when things go wrong for which MSPs need to implement robust controls across security and recovery capabilities supported by stringent SLAs and SLOs.

Key SLAs and SLOs involve RPO, RTO, and mean time to detect but increasingly will need service levels for AI such as agent state, workflow, and guardrails. This can be considered as three tiers of resiliency, each protecting against a different failure mode and each with its own way of measuring success that meet governance and business assurance requirements.

Attribute	Backup as a service	Disaster recovery as a service	Cyber resilience as a service
Protects against	**Data loss**	**Outage**	**An adversary**
Assumes	Infrastructure fails	Site fails	Attacker already inside; backups are a target
Measured by	Job success; RPO	Failover; RTO	Time to clean, verified recovery

IDC's digital sovereignty stack

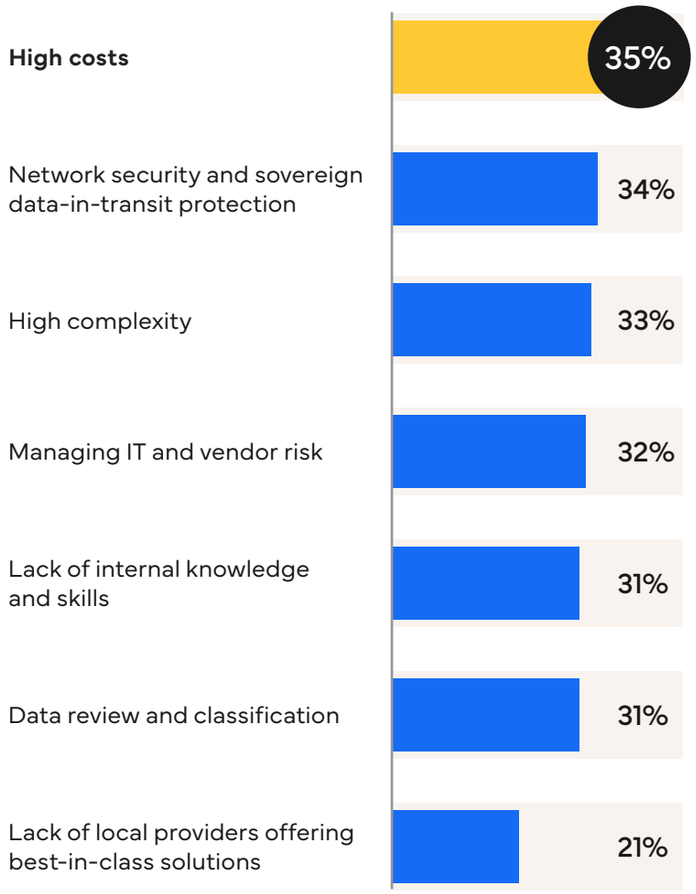
Cyber resilience is a response to an attack, not a discipline in its own right. In IDC's Digital Sovereignty Stack, it sits within the governance and business assurance layers, alongside data security, resiliency, and continuity. Sovereign hosting needs sovereign systems management, often via managed service providers.



Source: IDC's *Worldwide Digital Sovereignty Taxonomy*, 2026

Pain points: The differentiation opportunity

High costs rank as the top challenge in implementing sovereign cloud, with security, complexity, and vendor risk also critical. These pain points are the flip side of the opportunity: MSPs can create differentiated services that address them through cost and economic management, control and management planes, and co-management.



- **High costs are a challenge for 35%.** New tools for data management and specialist skills are the top areas where extra budget will be needed.
- Despite increasing interest in digital sovereignty, **most organizations aren't willing to allocate more than 6–10% of their cloud budgets to sovereign cloud solutions.**
- Sovereignty is not just about protecting data at rest or at work. **Sovereign control of data in transit is also a concern for 34%.** A lack of network operators capable of guaranteeing sovereign controls exacerbates this challenge.
- **High complexity begins from the outset of the digital sovereignty journey** as users need to review their data and classify it according to sensitivity. This is easier said than done, and is particularly challenging for those who have large and sprawling data sets, and/or lack the in-house expertise to manage that data.
- **Managing IT and vendor risk is the top obstacle for 32%.** This gives rise to a separate set of challenges: When asked what difficulties they face when diversifying their technology ecosystem to ensure digital sovereignty,* 39% identify high switching costs and contractual lock-in with their existing providers; 34% say it's regulatory and compliance constraints impacting diversification efforts; and 31% cite limited availability of local/regional technology providers.

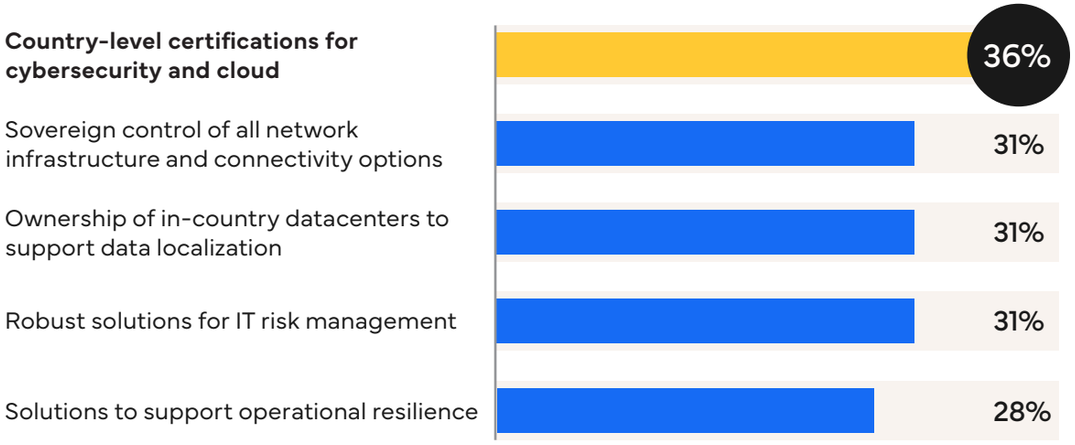
n = 633; Source: IDC's *Worldwide Digital Sovereignty Survey,* June 2026. n = 955 (*); Source: IDC's *Worldwide Digital Sovereignty Survey,* July 2025

What sovereign cloud customers are looking for

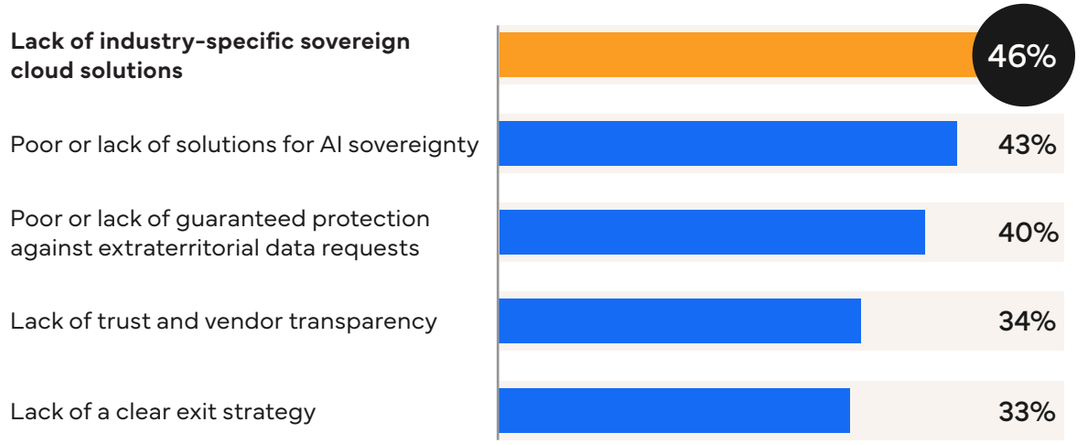
Sovereign cloud providers with cybersecurity certifications, network and risk management controls, and industry-specific and AI solutions are highly coveted.

Meeting these expectations requires MSPs to invest in critical capabilities spanning security certifications for sovereignty (e.g., NIS2, DORA, SecNumCloud); management planes supporting infrastructure; expertise, reference architectures, and frameworks of industries; and engineering expertise for AI and data.

Which attributes are important when choosing a sovereign cloud partner or provider?



Where do current offerings for digital sovereignty fall short?



n = 633; Source: IDC's *Worldwide Digital Sovereignty Survey,* June 2026

Aligning to regional rules: The EU's SEAL ratings

The European Commission has made sovereignty scorable through its Cloud Sovereignty Framework that describes five Sovereignty Effectiveness Assurance Levels (SEALs).

MSPs must have in-depth knowledge of SEAL to deploy sovereignty that ensures compliance and identify the proper level of deployment while providing key capabilities such as local operations, control planes, ecosystem and supply chain risk management, and increasingly automation, which is driven by complexity of compliance, scaling operations, and need to support vast resources including data as well as resiliency and assurance.

The Commission's Cloud Sovereignty Framework rates providers from SEAL-0 to SEAL-4 across eight sovereignty objectives, then combines them into a weighted score built from 48 criteria. Supply chain carries the heaviest weighting.

Level	What it means	What to expect buyers will want to see
SEAL-0	No sovereignty. Service, technology, and operations sit under non-EU control	Treat any sovereignty claim with caution
SEAL-1	Jurisdictional sovereignty	Governing law, contracting entity, dispute venue
SEAL-2	Data sovereignty. EU law applies and is enforceable without extra measures by the customer	Support model, staff location and employment, access logs
SEAL-3	Digital resilience. Service, technology, or operations immune from non-EU supply chain disruption	Subprocessor register, exit and portability plan, recovery test results
SEAL-4	Full digital sovereignty. A complete EU supply chain, from chips to software	Bill of materials, component provenance, ownership of the parent entity

The framework was first applied in the Commission's own sovereign cloud procurement in April 2026, worth up to €180 million over six years. SEAL-2 was the minimum eligibility threshold, and three of the four awarded consortia reached SEAL-3. IDC's view is that SEAL is a procurement instrument built for EU institutions rather than a certification scheme, and no score substitutes for independent verification. Even so, MSPs should expect buyers well beyond the EU public sector to ask where they sit.

Sources: *European Commission, Cloud Sovereignty Framework v1.2.1*, October 2025, and *Cloud Sovereignty Framework Implementation Guidance*, June 2026; IDC's *Worldwide Digital Sovereignty Taxonomy*, 2026

Essential guidance

Success factors for MSPs in assisting organizations with implementing digital sovereignty must focus on the following:

Emphasize strategic capabilities



Implement robust governance
Build governance structure supporting risk and compliance management; policy enforcement including policy as code for AI; IAM and workforce controls; data oversight including classification, lineage, loss prevention, and egress control; contract management with third parties; and increasingly a registry for AI agents and models with defined guardrails



Demonstrate services expertise
Highlight advisory and architectural services that showcase industry expertise and ability to align and configure workloads with the right deployment models as defined by jurisdictional policies as well as ongoing operations that support meeting SLOs and SLAs particularly RTOs and RPOs including model and agent recovery times



Incorporate critical competencies
Implement management and control planes to optimize performance; compliance engineering for regulations and policies; assurance that includes end-to-end security and recovery capabilities; and cost and economics management such as FinOps particularly for AI and data

Highlight knowledge of sovereignty



Know the full sovereignty stack
Cover all six dimensions (data, technical, operational, assurance, supply chain, and geopolitical), not just data residency, and be clear with customers on who is responsible for what



Know the local rules
Be fluent in the regulations and certifications of each jurisdiction served (e.g., in Europe, NIS2, DORA, SecNumCloud, and the EU's SEAL ratings); be precise about the footprint where sovereignty can credibly be delivered, and evidence every claim



Build sector and data skills
Offerings fail without industry expertise and data classification tailored to the customer's sector and jurisdiction, including for AI models and training data



Sustain compliance and skills
Treat sovereignty as an ongoing commitment, with continuous compliance and assurance, rapid adaptation as policies change, and continued investment in specialist skills and tools

About the IDC analysts



Rahiel Nasir

**Research Director and Lead Analyst,
Digital Sovereignty, IDC**

Rahiel Nasir is research director within IDC's enterprise infrastructure global research domain and part of the Cloud and Datacenters subdomain. Nasir is IDC's global lead on digital, cloud, and AI sovereignty. In this capacity, he covers emerging sovereignty initiatives and global market trends. Nasir provides insights into geopolitical shifts that affect infrastructure buying decisions, chief among them sovereign AI and cloud. Nasir developed IDC's first sovereign cloud taxonomy, market size, and forecast, and has co-developed the Sovereign AI Infrastructure Index, IDC's first market size and forecast that tracks worldwide spend on sovereign AI infrastructure.

More about Rahiel Nasir →



David Tapper

**Program Vice President,
Outsourcing and Managed Cloud Services, IDC**

David Tapper serves as program vice president for IDC's Outsourcing and Managed Cloud Services research team, which develops research for technology outsourcing and managed services, business process outsourcing, and global sourcing, also referred to as offshore/nearshore. As part of this research, the group covers emerging services areas such as mobility, social media, analytics, automation, IoT, and cloud services. Tapper also provides strategic thought leadership on the transformation of the services industry to newer models of delivery, including cloud computing, managed cloud services, and SaaS (software as a service).

More about David Tapper →

Message from the sponsor

COHESITY

Organizations pursuing sovereign cloud initiatives face a growing challenge: Protecting sensitive data while meeting increasingly complex requirements for security, resilience, and compliance. As trusted advisors, managed service providers play a critical role in helping customers navigate these demands and deliver secure, sovereign services with confidence.

Cohesity is a leader in AI-powered data security, cyber resilience, and data management, helping organizations protect, secure, and derive value from their most critical information. We enable MSPs to build and deliver sovereign cloud offerings that support customer requirements for data control, operational resilience, and regulatory compliance without compromising innovation or simplicity.

As this IDC research highlights, success requires a thoughtful approach that combines technology, expertise, and trusted partnerships. Cohesity is committed to empowering MSPs with the platform, programs, and support they need to help customers confidently adopt sovereign cloud strategies and protect their most sensitive data.

IDC Custom Solutions

IDC Custom Solutions produced this publication.
The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies.

This IDC material is licensed for external use and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

IDC.com | IDC on LinkedIn | IDC Blog

International Data Corporation (IDC) is the technology intelligence layer of the AI economy. A global leader in research and data for more than 60 years, IDC's expert analysts, proprietary datasets, and rigorous methodologies are trusted by business and IT leaders to guide critical business strategies and IT investments. Today, that intelligence is built into the tools and workflows where work gets done with IDC Quanta, making work sharper, teams faster, and businesses harder to beat.

©2026 IDC. Reproduction is forbidden unless authorized. All rights reserved. CCPA