March 2026
InfoBrief
Sponsored by Microsoft

Digital Sovereignty Reconsidered: From Location-Based Assurance to Enforceable Control

How Regulated Organizations Can Operationalize Sovereignty in a Cloud- and AI-Driven World

Ruthbea Yesner
Vice President,
Government Insights, Education, and Smart Cities, IDC

Table of contents

Click any title to navigate directly to that page.

In this InfoBrief

Why digital sovereignty is a strategic priority for regulated industries.

Organizations are shifting toward enforceable, auditable, and hybrid sovereignty models to manage data, AI, security, and resilience.

Organizations in regulated sectors such as energy, finance, healthcare, and government know that data and, increasingly, AI are core to competitiveness and security. This elevates the importance of protecting sensitive workloads and ensuring compliance. As cyber threats, geopolitical instability, and fragmented regulations grow, digital sovereignty becomes a strategic priority, shaping where data resides, who controls it, how AI is trained, and which technology partners can be trusted.

In this InfoBrief (continued)

IDC views sovereignty as a comprehensive governance discipline that spans data, technical, and operational domains.

It involves a spectrum of deployment options that organizations choose from to align with workload needs, data sensitivity, and regulatory obligations. Achieving sovereignty requires technically enforceable, continuously monitored, and independently verifiable controls. Organizations that prioritize these auditable controls are better equipped to meet regulatory scrutiny, manage operational risk, and build long-term digital resilience.

Decision-makers in regulated sectors increasingly see sovereignty not as a binary choice between global and local providers but as an evaluation of which platforms deliver the strongest mix of enforceable controls, transparency, resilience, AI innovation, and regulatory assurance for each workload. As a result, many organizations are adopting hybrid sovereignty strategies that combine mandated local requirements with hyperscale capabilities where security, resilience, and innovation are essential.

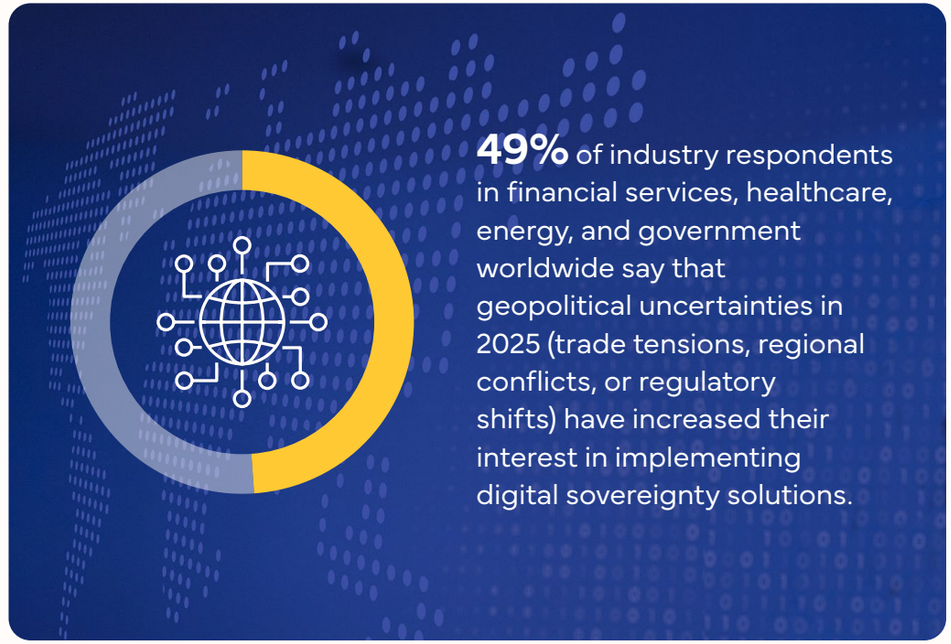
This InfoBrief leverages data from IDC's *2025 Worldwide Digital Sovereignty Survey,* global *2025 Government Industry Intelligence Survey,* and *Future Enterprise Resiliency and Spending* surveys, secondary research, and conversations with regulated industry organizations.

Why digital sovereignty has become a strategic priority

Sovereignty is now an executive-level issue tied to trust, continuity, and long-term digital competitiveness.

There are significant market forces driving urgency:

- Geopolitical uncertainty has heightened geopolitical risk and operational concerns around continuity, access, and control.
- Accelerating adoption of cloud-native and AI-driven services has increased exposure to cross-border data flows and operational dependencies.
- Increasing and overlapping government and industry regulatory requirements are expanding across data protection, AI governance, and cybersecurity.
- Rising expectations for transparency, auditability, and resilience are integral to customer and public trust and resilience.



Source: IDC's *Worldwide Digital Sovereignty Survey*, July 2025

Why digital sovereignty has become a strategic priority (continued)

What are, or were, the main drivers of your organization's decision to use sovereign cloud?

	Healthcare	Energy	Government	Financial services
Protect against extra-territorial data requests	37%	37%	36%	
Increase data privacy and security	36%		35%	
Comply with national/regional legislation	45%	37%		
Comply with industry regulations		41%		40%
Increase customer trust	35%			37%

Note: Multiple dichotomous table; totals will not sum to 100%. Source: IDC's *Worldwide Digital Sovereignty Survey*, July 2025

Redefining sovereignty to execute control over data, operations, and decision-making

Improve trust using evidence-based governance and shift focus from **where** data is hosted to **how** control is exercised and evidenced.

IDC defines **digital sovereignty** as "the capacity for digital self-determination by nations, organizations, and individuals." This means giving data owners full control over where their data is stored, processed, managed, and accessed — including the supporting infrastructure, such as datacenters, networks, and the personnel with access to them.

Sovereign cloud is a form of digital sovereignty, providing public or dedicated cloud environments designed to meet applicable data laws and regulatory requirements through enforceable controls over infrastructure, access and operations. It spans a range of deployment models and capabilities that organizations configure based on workload sensitivity, regulatory needs, and risk tolerance.

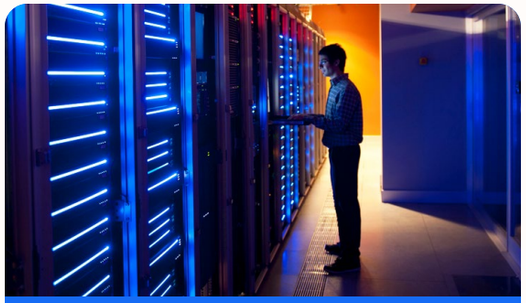
How does sovereign cloud fit into your organization's cloud strategy?

	Healthcare	Energy	Government	Financial services
Sovereign cloud is, or will be, a general part of our multicloud/hybrid-cloud strategy.	48%	62%	50%	57%
We use on-premises IT, and a sovereign cloud is, or will be, the only type of cloud we use.	45%	34%	40%	35%

Source: IDC's *Worldwide Digital Sovereignty Survey*, July 2025

Regulated buyers' sovereign cloud outcomes focus on security, control, access, and resilience

The main benefits of sovereign cloud demonstrate the scope of sovereignty decisions across data, technology infrastructure, and operations.



Data residency ensures locality of data, backups, and identity services.

Regulatory alignment improves compliance posture and audit readiness.

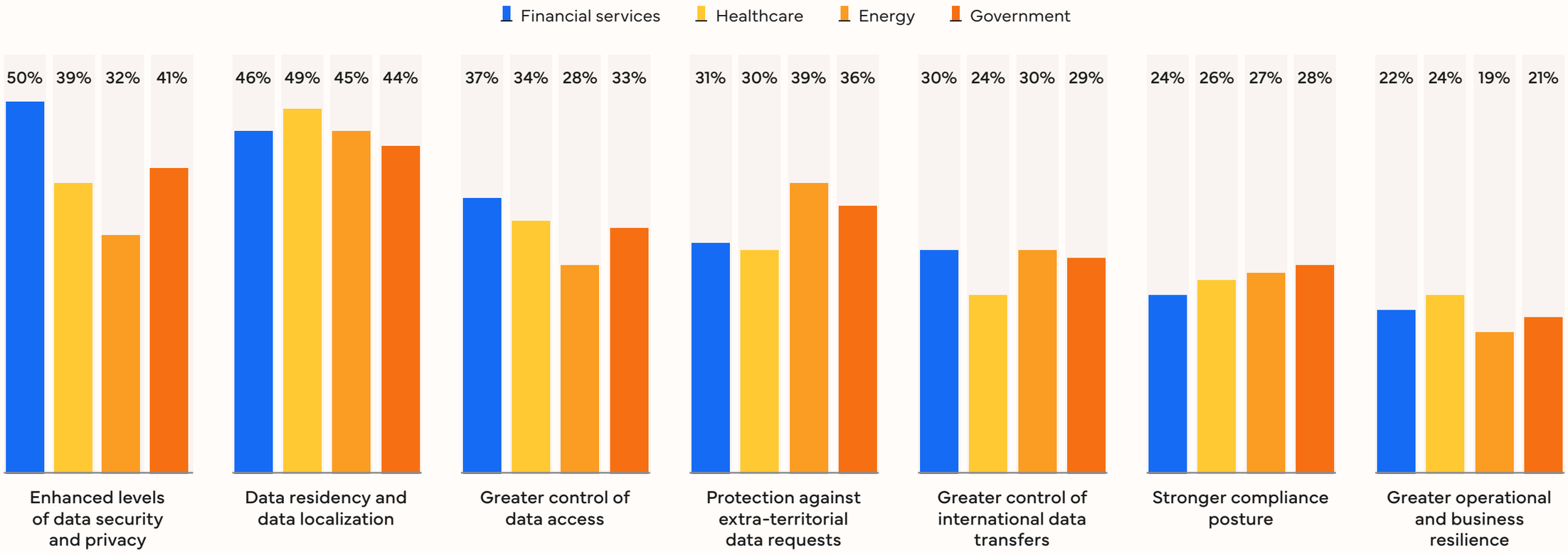
Access control provides protection from unauthorized access (including cloud provider access).

Business continuity and operational resilience sustain operations even during geopolitical or infrastructure disruption.

Regulated buyers' sovereign cloud outcomes focus on security, control, access, and resilience (continued)

What are the main benefits that sovereign cloud has brought, or could bring, to your organization?

See the figure data in an accessible table format.



Source: IDC's *Worldwide Digital Sovereignty Survey*, July 2025

From psychological discomfort to operational assurance

For industries with complex and sensitive data and stringent regulatory requirements, deciding how to deploy digital sovereignty can be more a matter of mindset than of technical and operational factors.

Sovereignty as a psychological and governance challenge

- Sovereignty concerns and buyer anxiety often reflect fear of losing agency and control, not just of meeting compliance requirements.
- Digital sovereignty strategies must address organizational confidence and compliance to build trust with suppliers and in solutions. Trust and confidence should come from governance transparency and auditability, not geography alone.
- Transparency, dashboards, and audit evidence build trust over time by providing the ability to explain governance to regulators and boards.

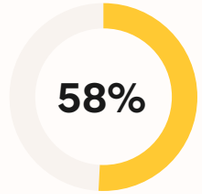
Source: IDC's *Worldwide Digital Sovereignty Survey*, July 2025

Sovereignty is not one-size-fits-all: A continuum approach

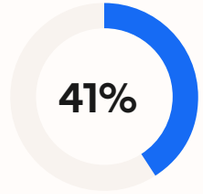
- Most regulated organizations require **multiple sovereignty postures within a single IT estate.**
- Most organizations adopt **multi-model sovereignty strategies.**
- Regulated organizations increasingly apply sovereignty by **workload and risk profile.**
- Sovereign public cloud capabilities address many regulatory and operational requirements.
  - Hybrid and disconnected environments support specialized or sensitive use cases.
  - National or partner-operated clouds remain essential where mandated.

Digital sovereignty challenges

Limited availability of local/regional technology providers



Energy



Government

Regulatory and compliance constraints impacting diversification efforts

Financial services and healthcare

Source: IDC's *Worldwide Digital Sovereignty Survey*, July 2025

Seek partners that can effectively enforce and prove sovereign controls over time

Hybrid sovereignty strategies that balance mandated local requirements with hyperscale capabilities where security, resilience, and innovation are critical.

Global hyperscalers offer scale in:

- Security depth
- Compliance engineering
- Operational maturity
- Resilience and continuity
- In-country datacenters and partners
- AI innovation

Consider global hyperscalers for workloads when:

- Resilience across multi-region operations within a single sovereignty boundary is required.
- Geopolitical, infrastructure, or connectivity disruptions need disaster recovery and crisis-tested operating models.
- Advanced tools are required to meet leadership mandates for technical and contractual enforcement of requirements.
- Workloads require advanced security and compliance engineering.

Seek partners that can effectively enforce and prove sovereign controls over time (continued)

Across regulated industries, the top attributes most important for choosing a digital sovereignty partner or provider are:

Ownership of in-country datacenters to support data localization

Sovereign control of all network infrastructure and connectivity options

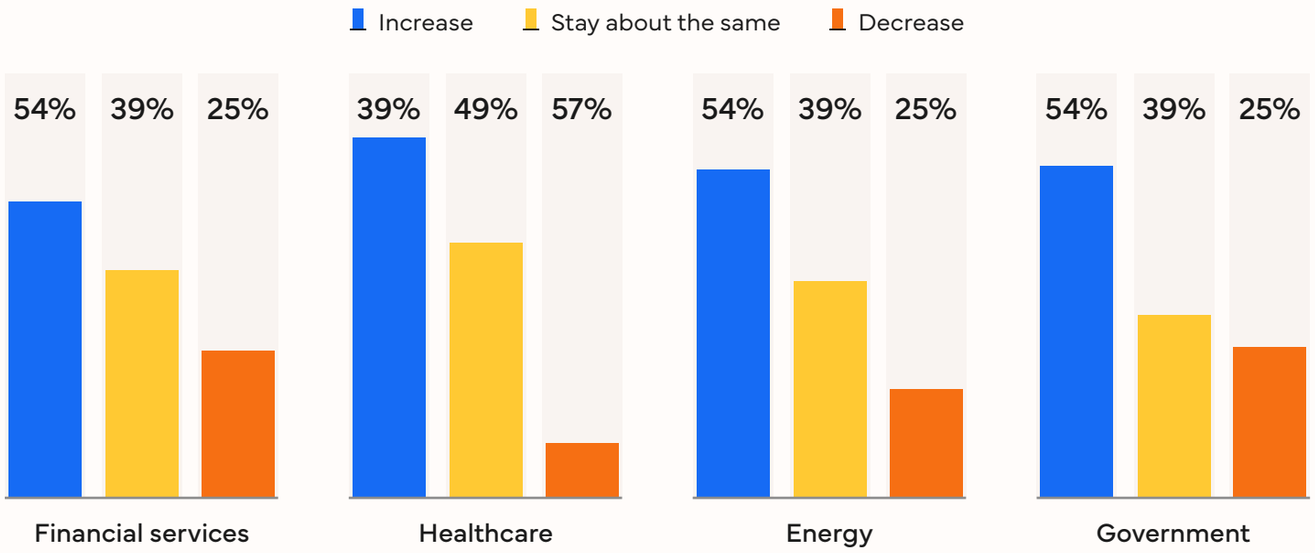
Country-level certifications for cybersecurity and cloud

Strong ecosystem of partners that adhere to sovereign principles

Policies and the need to control AI model governance will drive AI sovereignty use

How do you expect your organization's use of sovereign cloud for AI workloads to change over the next two years?

See the figure data in an accessible table format.



Reasons for the increase in use of sovereign cloud for AI workloads can vary by industry.

- **All regulated industries**
  Prioritize the desire to increase control over AI model governance and transparency.
- **Financial services (68%), healthcare (71%), and government (64%)**
  Cite the growing importance of national or local compliance requirements.
- **Energy (62%)**
  Emphasize continued geopolitical instability or trade restrictions as sovereign cloud drivers.

Source: IDC's *Worldwide Digital Sovereignty Survey*, July 2025

Cloud provider capabilities for a sovereign, AI-ready future

AI-focused security, compliance, data governance, and expertise rank among the top provider selection criteria, underscoring the need for transparent operations, customer-managed encryption keys, and confidential computing.

Leading cloud providers increasingly differentiate themselves by offering AI services that can be deployed within enterprise-controlled boundaries, while robust partner ecosystems add local regulatory expertise and implementation depth, critical for aligning AI adoption with sovereignty, trust, and operational resilience.

Criteria organizations use when selecting a cloud provider:

Europe

- 21% — AI offering on cloud provider's marketplace
- 22% — Specialized/AI-optimized hardware (e.g., GPUs and TPUs)
- 25% — Data governance and privacy features for AI workloads
- 25% — The availability of AI expertise and support from the provider
- 27% — AI-focused security and compliance offerings

Middle East, Turkey, and Africa

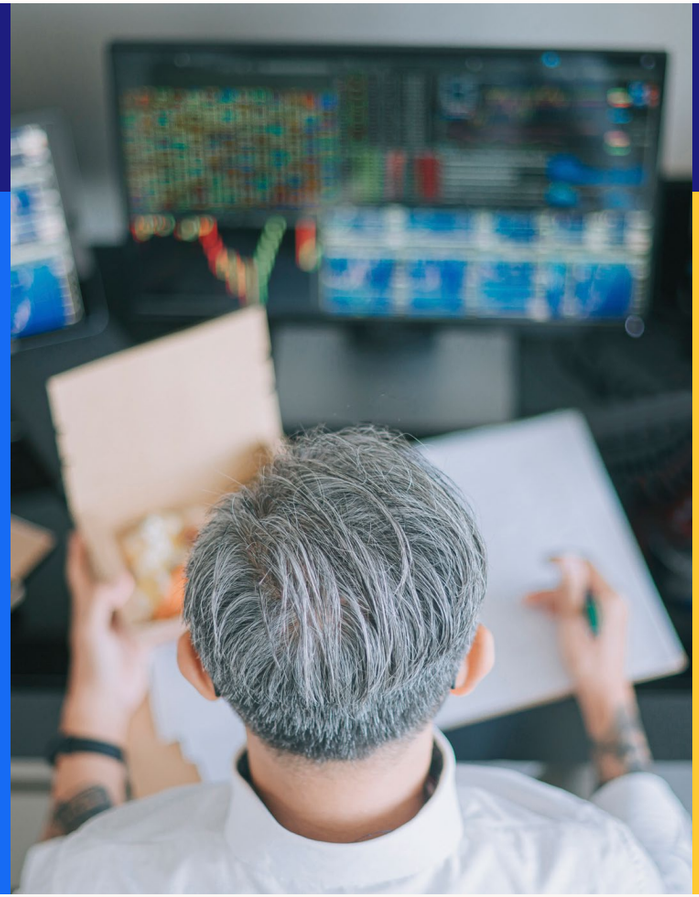
- 26% — AI-focused security and compliance offerings
- 26% — The availability of AI expertise and support from the provider
- 36% — The availability of AI expertise and support from the provider
- 37% — Integration with existing data pipelines and analytics tools
- 39% — Data governance and privacy features for AI workloads

n = 1,745 (n = 1155 Europe, n = 590 Middle East, Turkey, and Africa); Source: IDC's *EMEA Cloud Survey*, September 2025

Financial services buyers assess sovereignty: From jurisdiction anxiety to audit-ready control

Leading financial institutions increasingly prioritize:

- Verifiable access logging
- Continuous compliance evidence aligned with financial regulators
- Focus on cryptographic control, auditability and audit evidence, and supervisory assurance
- Use of hybrid sovereignty models to balance regulatory mandates with hyperscale capabilities such as customer analytics, risk modeling, and AI-driven insights



Top AI use case types that require sovereign cloud infrastructure:

- Handling personal identifiable information (e.g., customer profiling or HR analytics)
- Processing sensitive or regulated data (e.g., financial records, legal documents)
- Using AI in autonomous decision-making with legal or safety implications (e.g., fraud detection)

Financial services buyers assess sovereignty: From jurisdiction anxiety to audit-ready control (continued)

Sovereign AI snapshot

Most important data-related factor influencing decision to localize AI workloads in a sovereign cloud environment:

56% **Organizational policies on risk/compliance**

Key consideration to ensure transparency and accountability in AI systems hosted on sovereign clouds:

36% **Maintain full audit logs of model inference and decisions**

72% **Critical to fully control the data used to train or fine-tune AI models**

70% **Essential to fully control the AI models in use**

Source: IDC's *Worldwide Digital Sovereignty Survey*, July 2025

Government buyers assess sovereignty: Enable public trust and services continuity

Governments recognize that:

- Public trust depends on continuity of service and accountability, not just ownership
- Digital public services and critical infrastructure must remain operational during crises, elections, or geopolitical events
- Auditable governance and transparent oversight matter as much as physical location

Top AI use case types that require sovereign cloud infrastructure:

- Processing sensitive or regulated data (e.g., financial records, health data, or legal documents)
- Supporting critical infrastructure or national systems (e.g., energy grids, defense, or emergency services)

Government buyers assess sovereignty: Enable public trust and services continuity (continued)

Sovereign AI snapshot

Most important data-related factor influencing decision to localize AI workloads in a sovereign cloud environment:

49% **Avoid exposure to foreign government access or surveillance**

Key consideration to ensure transparency and accountability in AI systems hosted on sovereign clouds:

44% **Maintain full audit logs of model inference and decisions**

42% **Use explainable AI tools with documented decision logic**

74% **Critical to fully control the data used to train or fine-tune AI models**

73% **Essential to fully control the AI models in use**

Source: IDC's *Worldwide Digital Sovereignty Survey*, July 2025

Healthcare buyers assess sovereignty: Protect sensitive data while enabling innovation

As digital health and AI adoption accelerate, providers focus on:

- In-region (and AI) processing of clinical and insurance data, patient confidentiality and data protection, and AI governance
- Explicit controls over model training and data reuse
- End-to-end security across data pipelines, not just storage
- Retaining patient record systems in tightly controlled environments
- Use of hyperscale platforms with sovereign AI and data residency controls for diagnostics, population health analytics, and research

Top AI use case types that require sovereign cloud infrastructure:

- Processing sensitive or regulated data (e.g., financial records, health data, or legal documents)
- Using AI in public sector or government health projects
- Using AI in autonomous decision-making with legal or safety implications (e.g., medical triage)

Healthcare services buyers assess sovereignty: Protect sensitive data while enabling innovation (continued)

Sovereign AI snapshot

Most important data-related factor influencing decision to localize AI workloads in a sovereign cloud environment:

47% **Sensitivity of data types (e.g., personal, health, or financial)**

Key consideration to ensure transparency and accountability in AI systems hosted on sovereign clouds:

38% **Maintain full audit logs of model inference and decisions**

74% **Critical to fully control the data used to train or fine-tune AI models**

73% **Essential to fully control the AI models in use**

Source: IDC's *Worldwide Digital Sovereignty Survey*, July 2025

Energy buyers assess sovereignty: Support operational resilience

Utilities and critical infrastructure operators recognize that:

- Cyber-resilience and disaster recovery are sovereignty requirements
- Operational technology (OT) and IT convergence demands stronger security controls
- Local-only platforms may struggle to support large-scale monitoring, AI, and predictive maintenance securely

Energy organizations use a hybrid approach to:

- Keep operational control systems local or isolated and use hyperscale sovereign cloud services for analytics, grid optimization, and resilience planning

Top AI use case types that require sovereign cloud infrastructure:

- Supporting critical infrastructure or national systems (e.g., energy grids, defense, or emergency services)
- Processing sensitive or regulated data (e.g., customer utility bills, legal documents)

Energy buyers assess sovereignty: Support operational resilience (continued)

Sovereign AI snapshot

Most important data-related factor influencing decision to localize AI workloads in a sovereign cloud environment:

56% **Sensitivity of data types (e.g., personal, health, or financial)**

Key consideration to ensure transparency and accountability in AI systems hosted on sovereign clouds:

33% **Maintain full audit logs of model inference and decisions**

35% **Use explainable AI tools with documented decision logic**

47% **Prefer control but use third-party or externally hosted data when necessary**

41% **Prefer control but accept external dependencies when needed**

Source: IDC's *Worldwide Digital Sovereignty Survey*, July 2025

Essential guidance

Achieve trusted digital sovereignty through control, proof, and adaptability.

Treat digital sovereignty as a strategic imperative, especially for regulated industries where data and AI are central to security, compliance, and economic competitiveness.

Adopt a governance-led view of sovereignty, encompassing data sovereignty, technical controls, and operational and energy resilience, not just data location.

Apply sovereignty on a continuum, selecting deployment models based on workload sensitivity, regulatory exposure, and risk tolerance rather than a one-size-fits-all approach.

Prioritize enforceable and auditable controls over provider ownership or geography, including technical enforcement, continuous monitoring, and independent verification.

Evaluate providers by their ability to deliver transparency, resilience, and regulatory assurance for each workload, not by global versus local labels.

Plan for hybrid sovereignty strategies, combining mandated local environments with hyperscale platforms where advanced security, resilience, and innovation capabilities are required.

Don’t assume you have to give up on cloud modernization, innovation, and transformation efforts with sovereign cloud.

Appendix: Accessible data table

This appendix provides an accessible version of the data for any complex figures in this document. Click "Return to figure" to get back to the data figure.

Page 9 figure

What are the main benefits that sovereign cloud has brought, or could bring, to your organization?

Benefits	Financial services	Healthcare	Energy	Government
Enhanced levels of data security and privacy	50%	39%	32%	41%
Data residency and data localization	46%	49%	46%	44%
Greater control of data access	37%	34%	28%	33%
Protection against extra-territorial data requests	31%	30%	39%	36%
Greater control of international data transfers	30%	24%	30%	29%
Stronger compliance posture	24%	26%	27%	28%
Greater operational and business resilience	22%	24%	19%	21%

Source: IDC's *Worldwide Digital Sovereignty Survey*, July 2025

Return to figure

Appendix: Accessible data table (continued)

Page 14 figure

How do you expect your organization's use of sovereign cloud for AI workloads to change over the next two years?

Change over the next two years	Financial services	Healthcare	Energy	Government
Increase	44%	53%	49%	49%
Stay about the same	34%	38%	33%	28%
Decrease	22%	8%	16%	23%

Source: IDC's *Worldwide Digital Sovereignty Survey*, July 2025

Return to figure

About the IDC analyst

Ruthbea Yesner

Vice President, Government Insights, Education, and Smart Cities, IDC

Ruthbea Yesner is the global research lead and vice president of IDC's Government Insights, Education, Transportation, and Smart Cities practice. Ms. Yesner and her team provide research and advisory services to public sector organizations and IT vendors on technologies essential to government transformation. Ms. Yesner is an author, speaker, and collaborator with organizations around the world, as well as a pioneer in urban technology innovation. She launched the Smart Cities practice at IDC in 2010.

More about Ruthbea Yesner →

Message from the sponsor

Microsoft

As digital sovereignty requirements expand beyond data residency to encompass governance, security, and operational resilience, organizations are rethinking how control is exercised and demonstrated across cloud and AI environments. Regulated industries in particular face growing expectations for enforceable controls, transparency, and audit-ready assurance while still needing to innovate and operate at scale.

Microsoft supports digital sovereignty strategies that emphasize customer control, verifiable governance, and adaptability across diverse regulatory and risk profiles. By enabling organizations to apply sovereignty by workload, data sensitivity, and compliance needs, cloud platforms can help balance local requirements with the resilience and security capabilities required for modern digital operations.

Learn more about Microsoft's approach to digital sovereignty and how organizations can operationalize control and accountability in cloud and AI environments.

Microsoft Sovereign Cloud | Microsoft AI

IDC Custom Solutions

IDC Custom Solutions produced this publication.

idc.com @idc @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. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.