InfoBrief, sponsored by Google Cloud | September 2025

Choosing a Sovereign Cloud Solution

Rahiel Nasir
Research Director, European Cloud Practice, Lead Analyst, Digital Sovereignty, IDC

Massimiliano Claps
Research Director,
IDC Government Insights

Table of Contents

In This InfoBrief 3

What Is Digital Sovereignty? 4

Why Is It Important? 5

What Is Needed for Cloud Sovereignty? 6

Choosing a Sovereign Solution 7

How to Implement Sovereign Cloud 8

Challenges for Users to Overcome 9

AI & Sovereignty 10

Advice for Technology Decision-Makers & Buyers 11

Advice for Policymakers 12

About the Analysts 13

Message from the Sponsor 14

About IDC 15

In This InfoBrief

This InfoBrief empowers technology buyers to make strategic choices about sovereign cloud acquisition and implementation, and it helps policymakers to craft regulations and policies that foster economic growth, national security, and strategic autonomy in the current geopolitical uncertainty.

Key takeaways:

- Digital sovereignty has gained prominence due to data privacy, data protection, and cybersecurity concerns. While Europe leads the demand for sovereignty, interest is growing globally due to geopolitical volatility.
  - **37%** of organisations globally are currently using sovereign public cloud solutions; **44%** are planning to use them.
- The strategic value of AI has increased attention to sovereignty among both technology buyers and policymakers.
  - **48%** of technology buyers expect their organisation's use of sovereign cloud for AI workloads to increase over the next two years.
- Technology buyers should choose a combination of global and local sovereign cloud partners to enable them to maintain sovereignty while harnessing cloud's innovation potential.
- No two organisations are the same. After choosing the most suitable partners, organisations should tailor their approach to implementing cloud solutions to ensure such solutions meet their needs.

This InfoBrief is based on IDC's extensive research into digital sovereignty, drawing upon, among other sources, IDC's *Worldwide Digital Sovereignty Survey, 2025.*

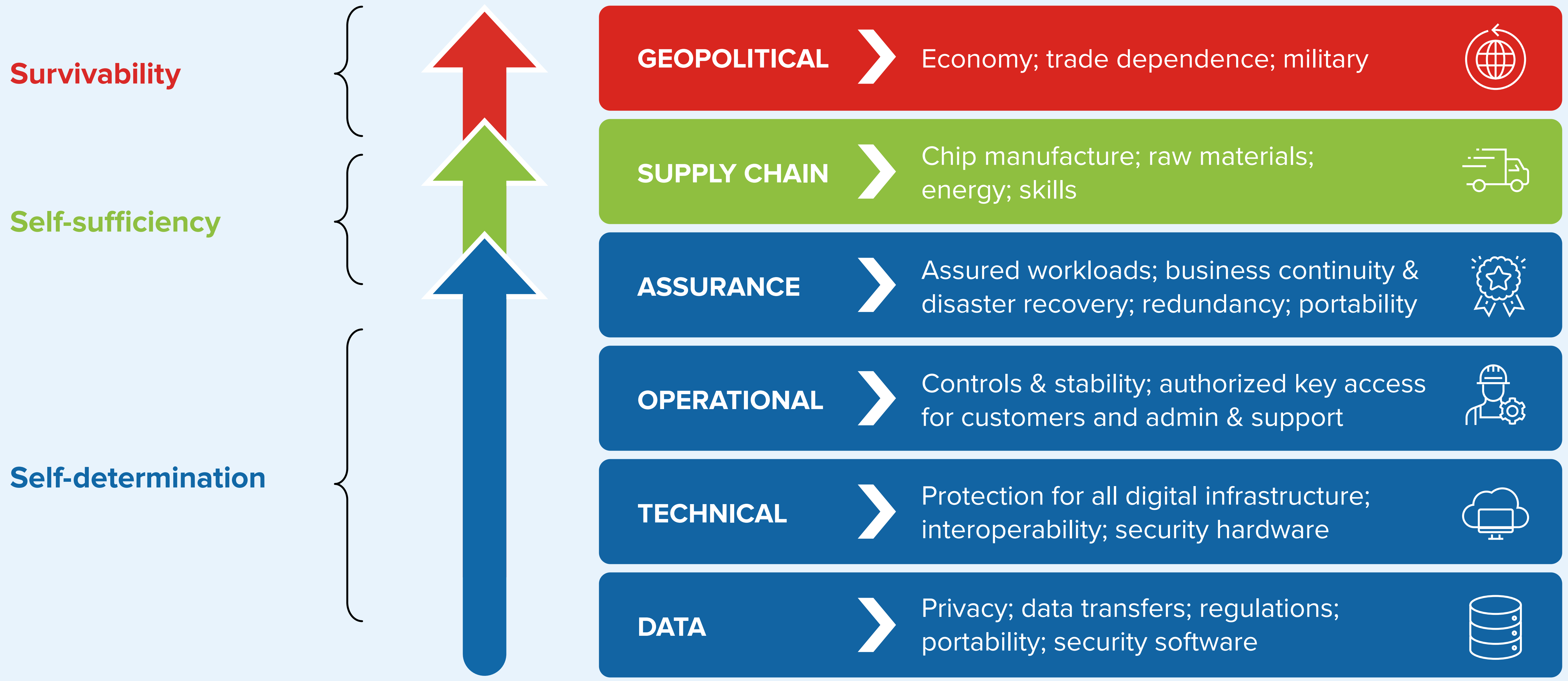
What Is Digital Sovereignty?

Digital sovereignty can be broadly defined as the capacity for digital self-determination by nations, companies, or individuals.

- This means giving data and system owners total control over how and where their data and systems are managed, stored, and processed by service providers.
- The above includes all the underlying infrastructure used for the data, such as data centres and networks, as well as all the support and admin staff who have access to that data and infrastructure.

IDC's Digital Sovereignty Stack

- The idea of digital sovereignty has gained traction in recent years amid increasing concerns around data privacy and protection.
- As the use of digital technologies pervades all aspects of society, digital sovereignty encompasses many attributes, shifting gear and emphasis from self-determination to self-sufficiency and the survivability of the end-to-end technology stack.



Survivability

- **GEOPOLITICAL** Economy; trade dependence; military

Self-sufficiency

- **SUPPLY CHAIN** Chip manufacture; raw materials; energy; skills

Self-determination

- **ASSURANCE** Assured workloads; business continuity & disaster recovery; redundancy; portability
- **OPERATIONAL** Controls & stability; authorized key access for customers and admin & support
- **TECHNICAL** Protection for all digital infrastructure; interoperability; security hardware
- **DATA** Privacy; data transfers; regulations; portability; security software

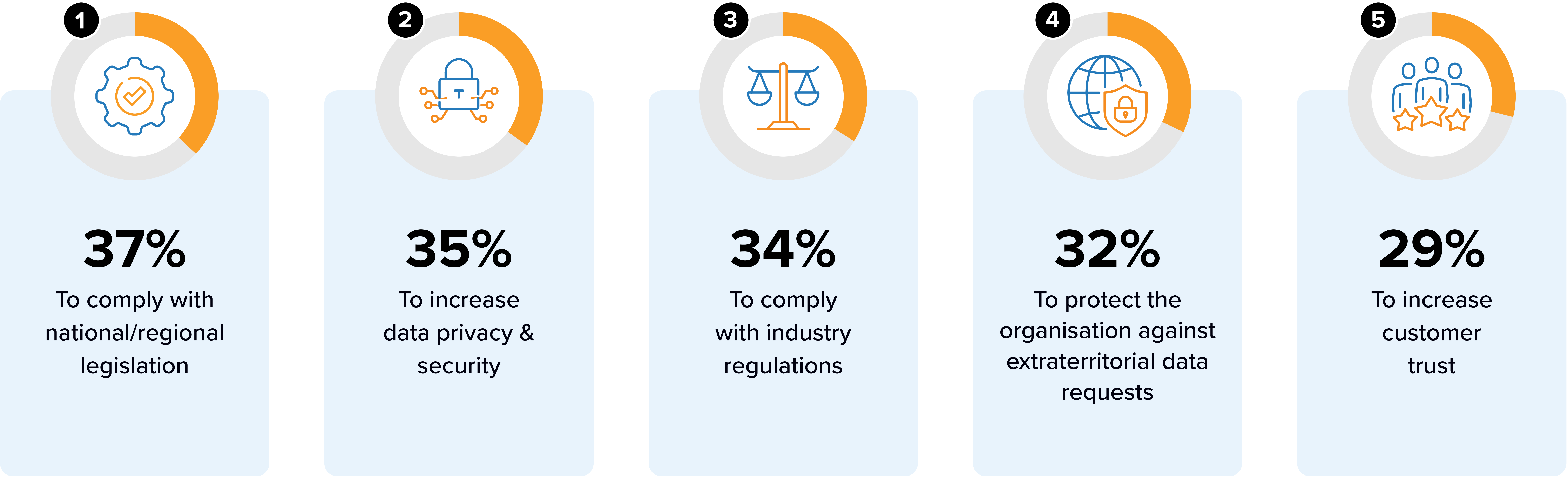
Source: IDC's *Worldwide Sovereign Cloud Taxonomy, 2024* (IDC #US50699324)

Why Is It Important?

37% *of organisations globally are currently using sovereign public cloud solutions.*

44% *are planning to use them in the future.*

The top five drivers for using sovereign cloud:



1 **37%** To comply with national/regional legislation

2 **35%** To increase data privacy & security

3 **34%** To comply with industry regulations

4 **32%** To protect the organisation against extraterritorial data requests

5 **29%** To increase customer trust

As digital laws and regulations continue to be enacted in markets around the world, many organisations need to ensure compliance with the rules or they will face harsh financial penalties, as well as potential long-term reputational damage, for any data breaches.

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

What Is Needed for Cloud Sovereignty?

As a foundation of digital business development, cloud is at the core of digital sovereignty development. Cloud sovereignty (or sovereign cloud) can be considered a subset of digital sovereignty.

A sovereign cloud comprises various solutions and technologies that all require strict controls to achieve three key levels of sovereignty:

1. **Data sovereignty:** IT and services that provide a holistic view of how data is collected, classified, processed, stored, managed, and monitored to ensure that regulatory compliance is always met
2. **Technical sovereignty:** controls applied to all digital infrastructure and services used for cloud-based data and workloads
3. **Operational sovereignty:** ensuring the transparency of all solutions that control cloud operations, from provisioning and performance management to monitoring physical and digital access to infrastructure

The main technology components needed to ensure cloud sovereignty:

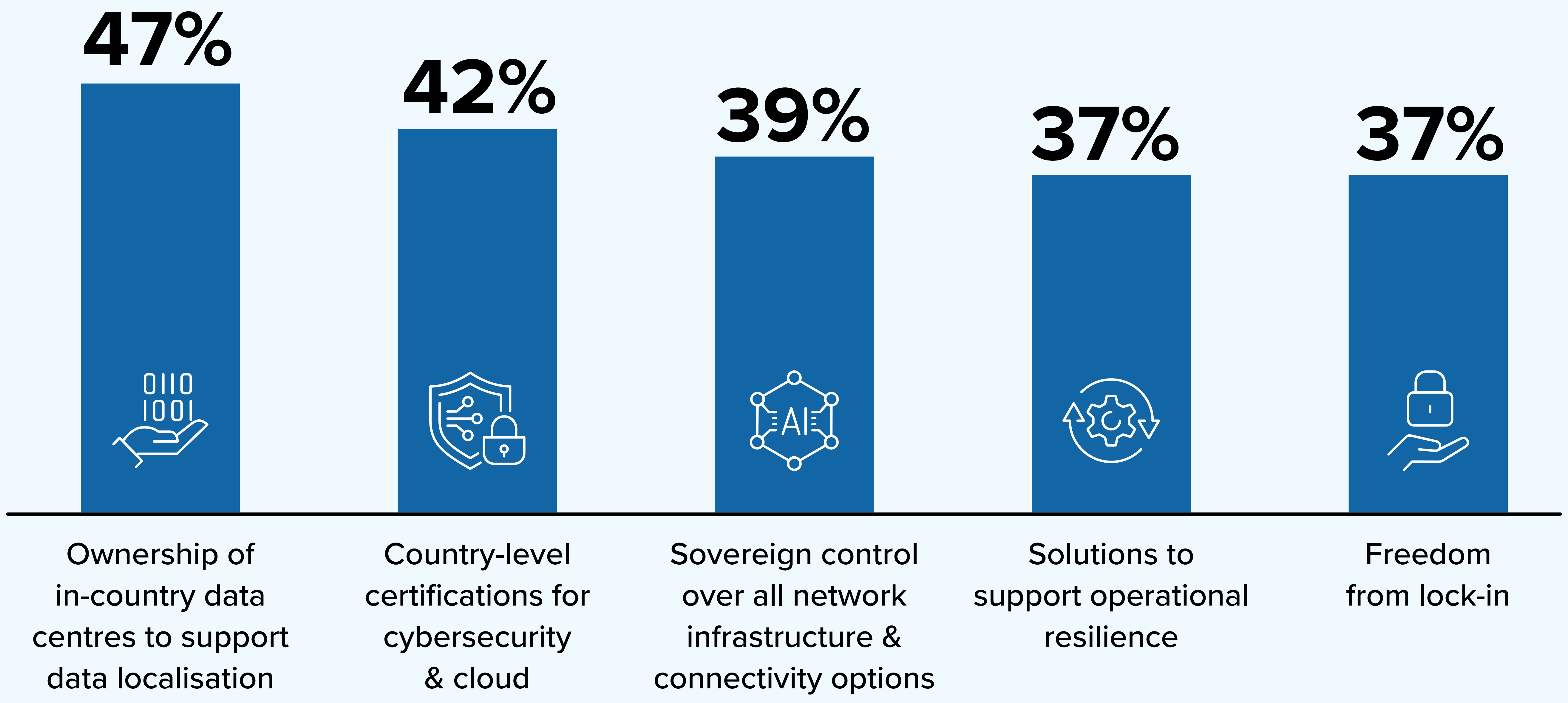
Data Sovereignty	Technical Sovereignty	Operational Sovereignty
IaaS data storage	Integrated infrastructure	Network equipment
PaaS	Systems infrastructure software	System and service management
Information and data security	Security hardware	Security analytics

Source: IDC's *Worldwide Sovereign Cloud Taxonomy, 2024* (IDC #US50699324)

Choosing a Sovereign Cloud Solution

Many cloud vendors and service providers have launched various solutions for digital sovereignty. Organisations should choose the solutions and services that meet their needs; one size does not fit all.

The top five attributes users look for when choosing a sovereign cloud partner:



What are the main benefits organisations aim to achieve by implementing sovereign cloud solutions?

43%	Data residency & data localisation
41%	Enhanced levels of data security & privacy
35%	Protection against extraterritorial data requests
34%	Greater control over data access
26%	Greater control over international data transfers
27%	Stronger compliance posture

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

How to Implement Sovereign Cloud

Data that is subject to regulatory compliance and/or is highly sensitive should be considered for sovereign cloud, as not all workloads need to be migrated. When deploying solutions, users should consider the following steps:

- **Review** security & compliance processes, tools, and skills.
- **Classify** data & apps by sovereignty requirements & workloads.
- **Control** the sovereignty of the classified data and apps.
- **Develop** specific programs to enable you to execute on sovereignty.
- **Balance** sovereignty requirements with innovation needs.
- **Maintain** security and compliance processes.

The main workloads that organisations expect to migrate to sovereign cloud:

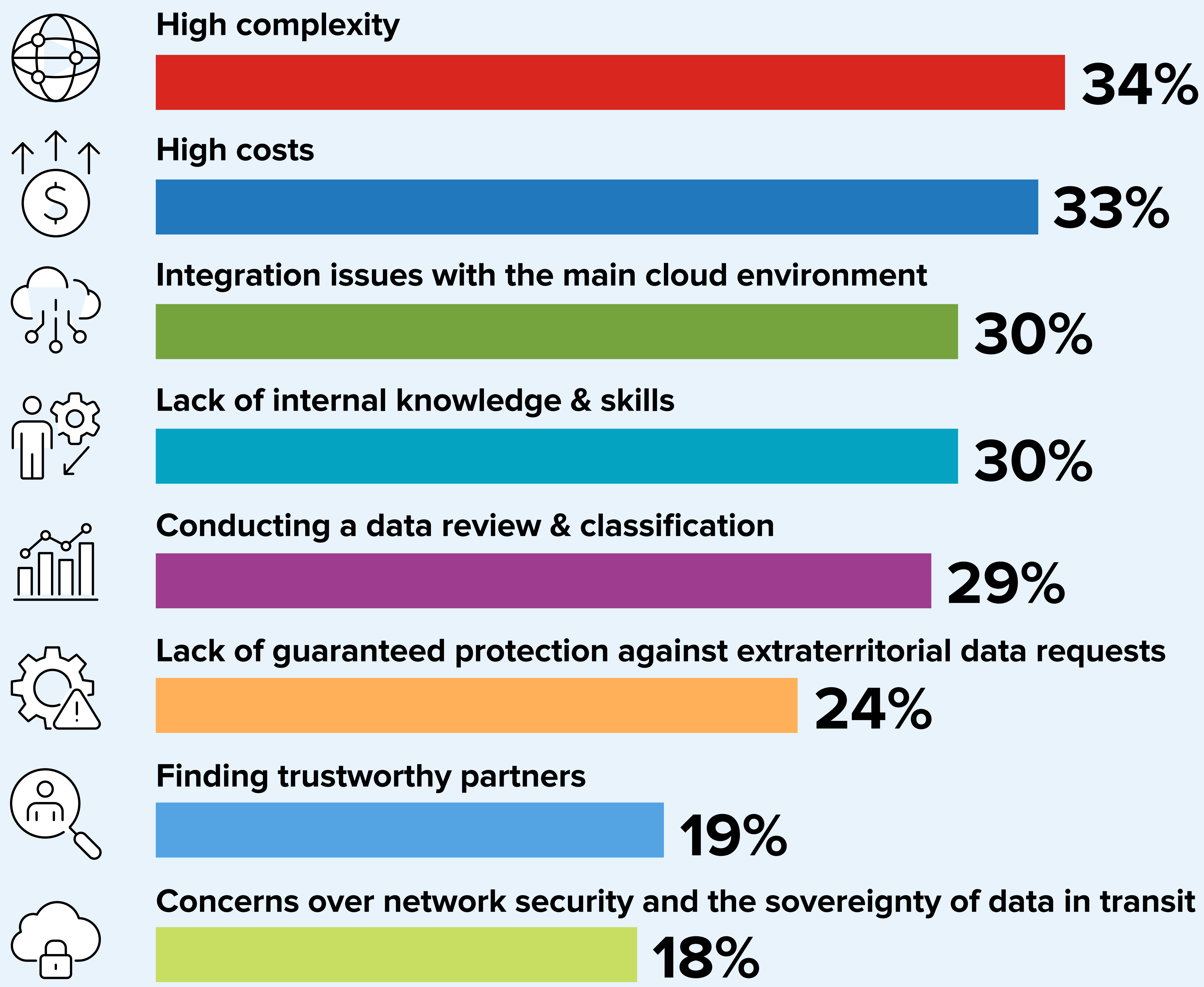
32%	Back-up/Recovery (IaaS)
31%	Data management (PaaS)
27%	Back-end business apps (SaaS)
26%	Storage (IaaS)
21%	App development (PaaS)
20%	Computing (IaaS)

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

Challenges for Users to Overcome

The top two obstacles that users often face when implementing sovereign cloud solutions are high complexity and high costs.

- **High complexity** includes challenges around data classification and identifying the full set of data and workloads that will be subject to sovereign requirements, integrating them into the main IT environment, and knowing what is needed for sovereignty.
- **High costs** typically include extra investments for local infrastructure & platforms, new tools for data governance & management, redesigning internal processes & mechanisms to ensure compliance, and skills & expertise.

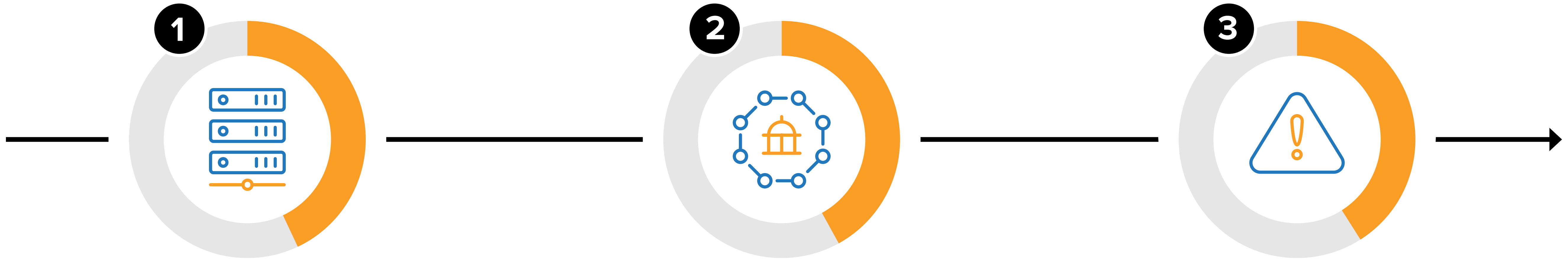


Source: IDC Europe's *Worldwide Digital Sovereignty Survey, 2025*, July 2025

AI & Sovereignty

The use of sovereign clouds for AI is increasing due to expanding compliance requirements.

The three most important data-related factors that influence an organisation's decision to localise AI workloads in a sovereign environment:



43%
The sensitivity of data types (e.g., personal, health, or financial)

42%
Data residency requirements under local law

41%
Organisational policies on risk & compliance

Organisations consider various factors to decide which AI workloads should be deployed in a sovereign cloud. Their top criterion is based on the sensitivity or classification of the data used. This is followed by regulatory or contractual obligations and internal AI governance or risk policies.

Does your organisation use, or plan to use, sovereign cloud to build AI solutions?

39%
Already using sovereign cloud to build AI solutions

27%
Not currently using but planning to do so within 12 months

48% expect their organisation's **use of sovereign cloud for AI** workloads to **increase** over the next two years.

58% say this increase is due to the **growing importance** of national or local **compliance requirements**.

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

Advice for Technology Decision-Makers & Buyers

Choose the right IT venue for your workloads.

Not all workloads need to be migrated to a sovereign cloud. Organisations should classify their workloads according to compliance requirements and the sensitivity of the data used. An appropriate solution for digital sovereignty should then be considered for this data.

Work with expert partners to help deal with the pain-points.

Organisations must be prepared to address challenges such as high complexity, high costs, and a lack of skills and knowledge when implementing sovereign solutions.

Stay ‘glocal’.

Partnerships with global and local providers are vital for sovereignty to work at scale, as well as to help maintain sovereignty while harnessing cloud’s innovation potential.

Share the responsibility of security.

Maintaining and monitoring cybersecurity and regulatory compliance are vital and must be an ongoing responsibility shared between all partners. Providers will be responsible for the security *of* the cloud, while users must take care of security *in* the cloud.

Beware of vendor lock-in.

Solutions that lead to vendor lock-in will restrict the ability to move workloads to the most appropriate IT venue. Open-source solutions should be considered to support data manoeuvrability, interoperability, and portability.

Look for sovereign network providers.

Sovereign controls should be applied not only to data at rest but also to data in transit.

Advice for Policymakers

Map the external risks.

Start with geopolitical volatility, intended economic competitiveness, and national security goals. A thorough and dynamic analysis will enable the definition of potential scenarios that inform policy choices.

Look at all aspects of digital sovereignty.

From data, technical, operational, and assurance requirements to supply chains and geopolitics, all attributes of digital sovereignty are intertwined and should be considered to ensure regulations are effective.

Learn from other jurisdictions.

Investigate the digital sovereignty regulatory landscapes that other countries are implementing to look for lessons learned (and pitfalls to avoid).

Do not limit regulatory analysis to data protection and cybersecurity.

Also consider the broader scope of AI strategies and action plans, energy resilience, sustainability strategies, intellectual property regulations, and public procurement regulations.

Invest in literacy and talent development.

Policymakers play a pivotal role in providing funding programs and creating public-private academic collaborations that can accelerate talent generation for innovation areas such as cloud, AI, and cybersecurity.

Educate the ecosystem.

Activating forums and committees will help other policymakers, private sector CIOs/CTOs/CAIOs, academic experts, and technology suppliers to understand the impacts of digital sovereignty regulatory interventions on both IT demand and IT supply.

About the Analysts

Rahiel Nasir,
Research Director, European Cloud Practice, Lead Analyst, Digital Sovereignty, IDC

UK-based Rahiel Nasir is responsible for co-leading and contributing to IDC's European Cloud Strategy research practice and also leads IDC's Worldwide Digital Sovereignty research programme.

Rahiel has been monitoring technology markets and writing about them throughout his professional life.

Prior to joining IDC, Rahiel was a research analyst, focused on the data centre infrastructure and services markets across the EMEA region, and a journalist, a role in which he edited several leading magazines covering the enterprise and consumer technology markets.

More about Rahiel Nasir

Massimiliano Claps,
Research Director, IDC Government Insights

Massimiliano (Max) Claps' research empowers technology suppliers and public sector professionals to embrace disruptive technologies such as AI, edge computing, and cloud to realise the benefits of strategic initiatives, including smart cities and citizen-centric government services.

Max is IDC Europe's lead analyst for passenger transportation, advising stakeholders across the transportation ecosystem on topics such as mobility as a service and intelligent traffic management. In addition, Max co-leads IDC's EMEA Cross-Industry Strategies and Use Cases thought leadership research.

More about Massimiliano Claps

Message from the Sponsor

Google Cloud

Organisations adopting cloud services operate within a landscape of evolving regulations and geopolitical factors that affect data residency, access, and control. Market requirements for digital sovereignty are diverse, and a single technical approach may not be suitable for all use cases.

Google Cloud provides a portfolio of solutions to offer choice without compromising functionality or innovation. Sovereign Cloud from Google offers a range from software-defined controls over the public cloud (Google Cloud Data Boundary) to partner-operated instances (Google Cloud Dedicated) and fully disconnected deployments (Google Cloud Air-Gapped). This range of options enables customers to meet their sovereignty needs workload by workload.

Learn more

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.

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 help IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.), the world's leading tech media, data, and marketing services company.

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. IDC's Custom Solutions group helps clients plan, market, sell, and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC

IDC UK
1st floor, Whitfield Street, London, W1T 2RE, United Kingdom
T 44.208.987.7100

@idc   @idc   idc.com