White Paper, sponsored by Google Cloud
SEPTEMBER 2025

The Strategic Importance of Digital Sovereignty

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

Massimiliano Claps
Research Director,
IDC Government Insights

Table of Contents

CLICK BELOW TO NAVIGATE TO EACH SECTION IN THIS DOCUMENT.

Executive Summary

Digital sovereignty has gained prominence due to growing concerns around data privacy, data protection, and, more recently, geopolitical risks. It is a broad concept that aims to give data owners full control and autonomy over their digital assets and infrastructure. While Europe leads the demand for digital sovereignty solutions, interest is growing globally due to rising cyberthreats and geopolitical uncertainties.

There are various aspects to digital sovereignty, including data, technical, operational, assurance, supply chain, and geopolitical sovereignty. Sovereign cloud can be considered a subset of digital sovereignty. Key drivers for adopting sovereign cloud include regulatory compliance, enhanced data privacy and security, and protection against extraterritorial data requests.

With nations now leveraging AI to achieve economic competitiveness and national security goals, AI sovereignty has emerged as another digital sovereignty subset. Sovereign controls across the AI stack, including data, models, and infrastructure, are vital to protect organisations against risks and ensure resilience.

Challenges in implementing sovereign cloud include high costs, complexity in data classification and integration, and a shortage of specialised skills. Trustworthy partnerships with global and local providers are essential to help overcome these challenges, as well as to ensure sovereignty at scale while balancing innovation and control.

It should also be borne in mind that not all organisations are the same and will therefore need sovereign solutions that meet their individual needs. When implementing sovereign cloud, organisations and policymakers are advised to adopt a tailored approach, focusing on workloads subject to regulatory and legal compliance and featuring high-sensitivity data. Major global and local cloud providers offer diverse options, including public cloud with sovereign controls and air-gapped environments. Organisations should prioritise flexibility, transparency, and expertise when selecting partners to ensure successful implementation and long-term compliance.

Once successfully deployed, a digital sovereignty solution can yield many benefits for users, such as greater data control, enhanced cybersecurity, operational resilience, and competitive advantages through increased customer trust.

In This White Paper

This IDC White Paper targets IT decision-makers, C-suite executives, and policymakers seeking to understand the complexities of digital sovereignty and what is needed to implement a solution. It defines the concept of digital sovereignty and its associated subsets, such as sovereign cloud and sovereign AI. The paper describes the current digital sovereignty landscape amid growing geopolitical uncertainties, what is driving the market, and what customers need to look for when choosing and using digital sovereignty solutions.

Unless otherwise indicated, all data sources used in this report are taken IDC's *Worldwide Digital Sovereignty Survey, 2025*.

The Digital Sovereignty Landscape

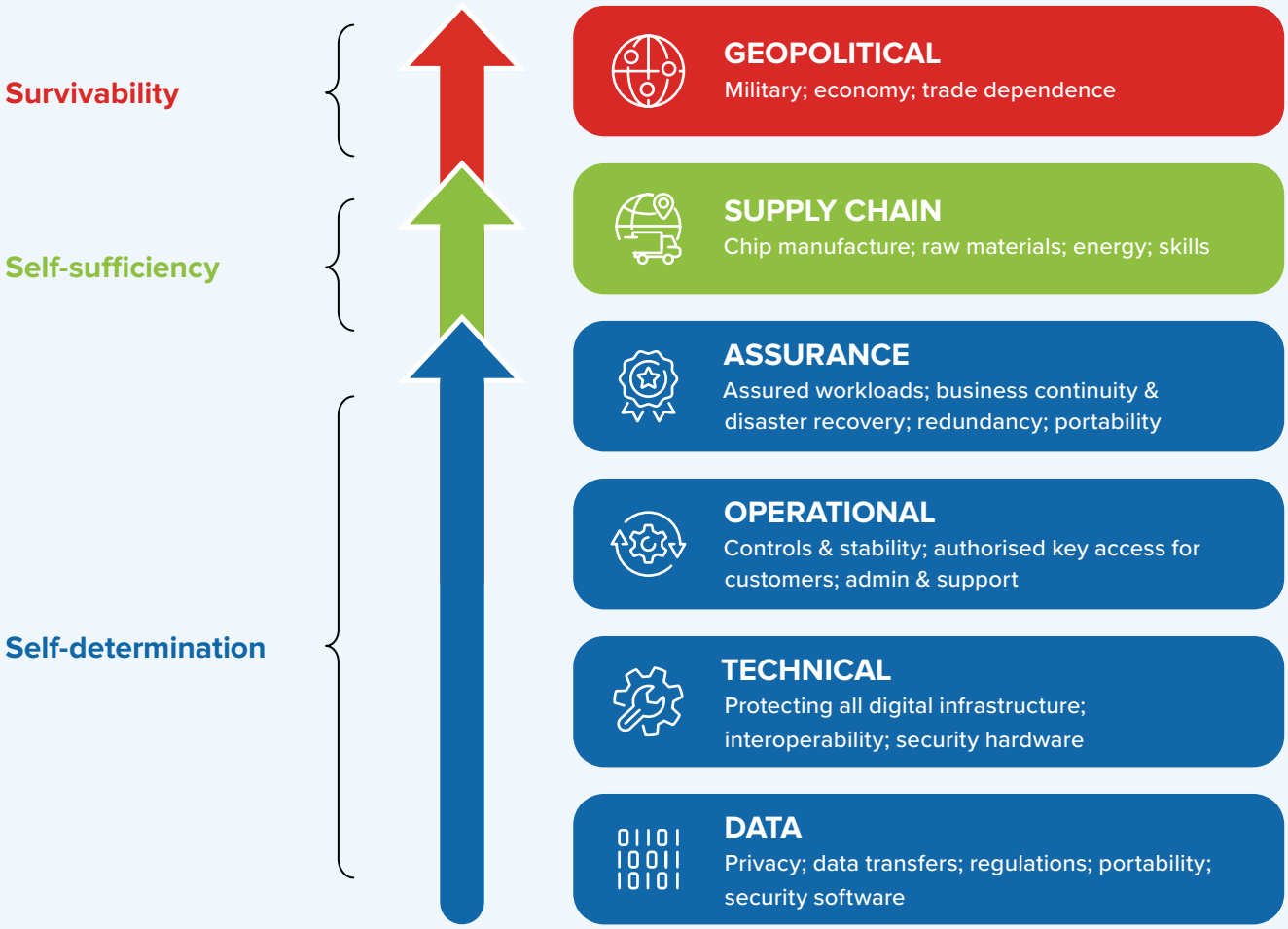
What Is Digital Sovereignty?

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

In essence, 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. This includes all underlying infrastructure used for the data, such as data centres and networks, as well as support and admin staff with access to that data and infrastructure.

The idea of digital sovereignty has gained traction in recent years amid increasing and ongoing concerns around data privacy and protection, especially as the use of digital technologies pervades all aspects of society. As a result, digital sovereignty encompasses many attributes, shifting gear and emphasis from data location and residency to self-determination, self-sufficiency, and the survivability of the end-to-end technology stack, as shown in Figure 1.

FIGURE 1:
Attributes of Digital Sovereignty



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

IDC considers data sovereignty a subset of the overall concept of digital sovereignty. Personal data privacy laws – such as the General Data Protection Regulation (GDPR) enacted across the European Union in 2018, India's Digital Personal Data Protection Act, which came into effect in 2023, and Saudi Arabia's Personal Data Protection Law, which has been in full force since 2024, among

others – typically kickstart the journey to digital sovereignty. This requires solutions for data sovereignty. Here, organisations look for 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.

Sovereign cloud can be regarded as another subset. As the foundation of digital business innovation, cloud will be at the core of digital sovereignty developments. As the use of digital technologies such as cloud computing expands and organisations move up the stack, they will require sovereign controls of solutions to achieve other aspects of sovereignty:

- **Technical sovereignty:** This refers to digital infrastructure located in a sovereign environment. It includes data centres plus all servers, other IT hardware, software, and everything as a service (XaaS) used for cloud-based data and workloads. All this infrastructure should be shielded from non-sovereign digital infrastructure and protected from all extra-territorial interference and scrutiny.
- **Operational sovereignty:** This includes solutions that offer cloud capabilities to enable transparency in controlling operations, from provisioning and performance management to monitoring physical and digital access to the infrastructure.

Data sovereignty, operational sovereignty, and technical sovereignty can be regarded as foundational pillars for building a sovereign cloud solution.

Beyond these three attributes, IDC's digital sovereignty model includes:

- **Assurance sovereignty:** This focuses on data availability and is essentially all about resilience. For example, in Europe, this is mandated by rules such as the Digital Operational Resilience Act (DORA), which defines the principles to ensure digital infrastructure across the continent's finance sector is always available to provide critical services.
- **Supply chain sovereignty:** Aside from reinforcing digital supply chain resilience, the aim here is to strengthen a digital economy's competitiveness, capacity to innovate, and ability to create jobs. Skills sovereignty – a nation's workforce capabilities to support all its digital ambitions – can also be considered a part of this layer.
- **Geopolitical sovereignty:** This takes the idea of digital sovereignty to a macro level. With IT and digital technologies now at the heart of a nation's critical infrastructure, governments must use technology solutions to help protect themselves against strategic weaknesses, vulnerabilities, and the high-risk dependencies of an increasingly volatile geopolitical environment. For instance, the White House 2025 Executive Order on Sustaining Select Efforts to Strengthen the Nation's Cybersecurity calls for, "actions to improve our nation's cybersecurity, focusing on defending our digital infrastructure, securing the services and capabilities most vital to the digital domain, and building our capability to address key threats."

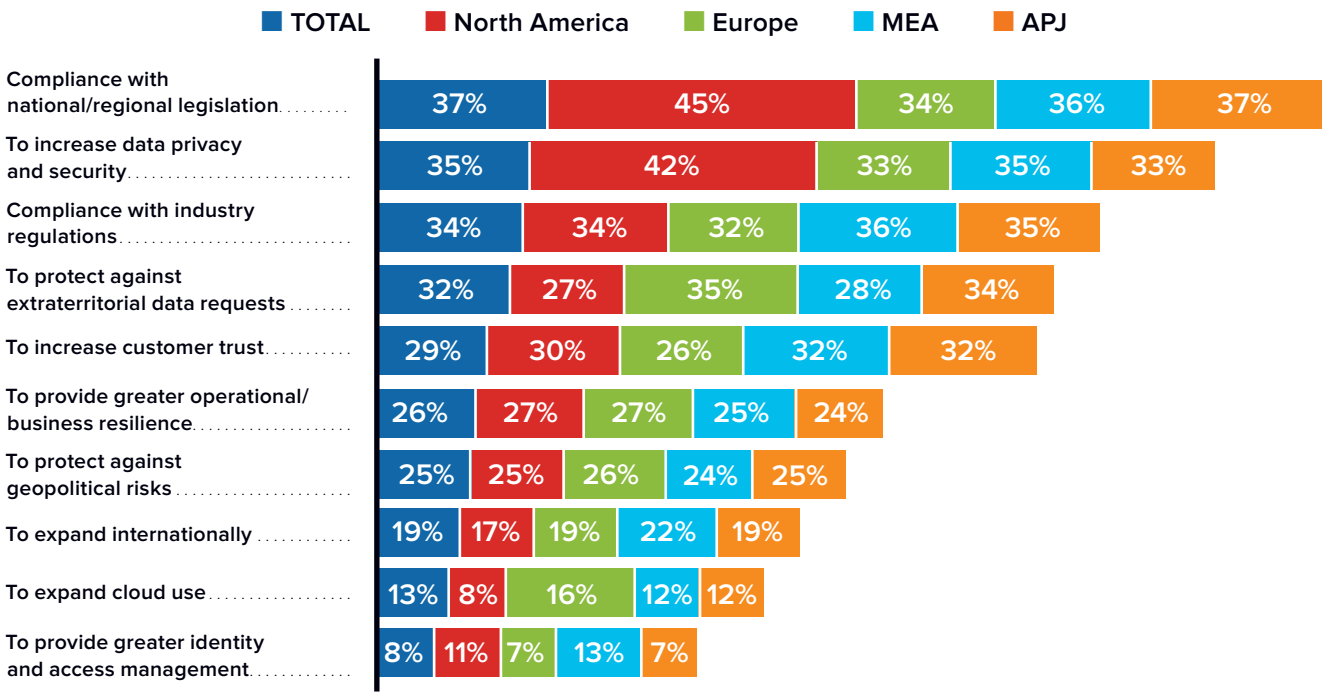
More recently, a third subset of digital sovereignty has emerged: AI sovereignty. From the United States' AI Action Plan and the EU's AI Continent Action Plan to Saudi Arabia's National Strategy for Data & AI, Japan's AI Promotion Act, and the Abu-Dhabi government's Digital Strategy 2025–2027, policymakers have earmarked AI as a strategic lever to achieve economic competitiveness, digital leadership, and strategic national security goals. From an economic competitiveness perspective, these initiatives aim to promote national AI innovation ecosystem growth and ensure the resilience of AI supply chains. From a national security perspective, policymakers consider AI a means to protect their countries from kinetic and non-kinetic threats. Achieving this requires the application of sovereign controls across the whole AI stack, from end to end, as shown in Figure 1. This includes safeguarding supply chain sovereignty for crucial resources, such as GPUs, chips, AI models, and talent.

Digital Sovereignty Market Drivers

IDC's *Worldwide Digital Sovereignty Survey, 2025* shows that compliance with industry regulations and compliance with national/regional legislation remain among the top three drivers for organisations seeking solutions for digital sovereignty, such as sovereign cloud (see Figure 2).

FIGURE 2:

The Drivers of an Organisation's Decision to Use Sovereign Cloud



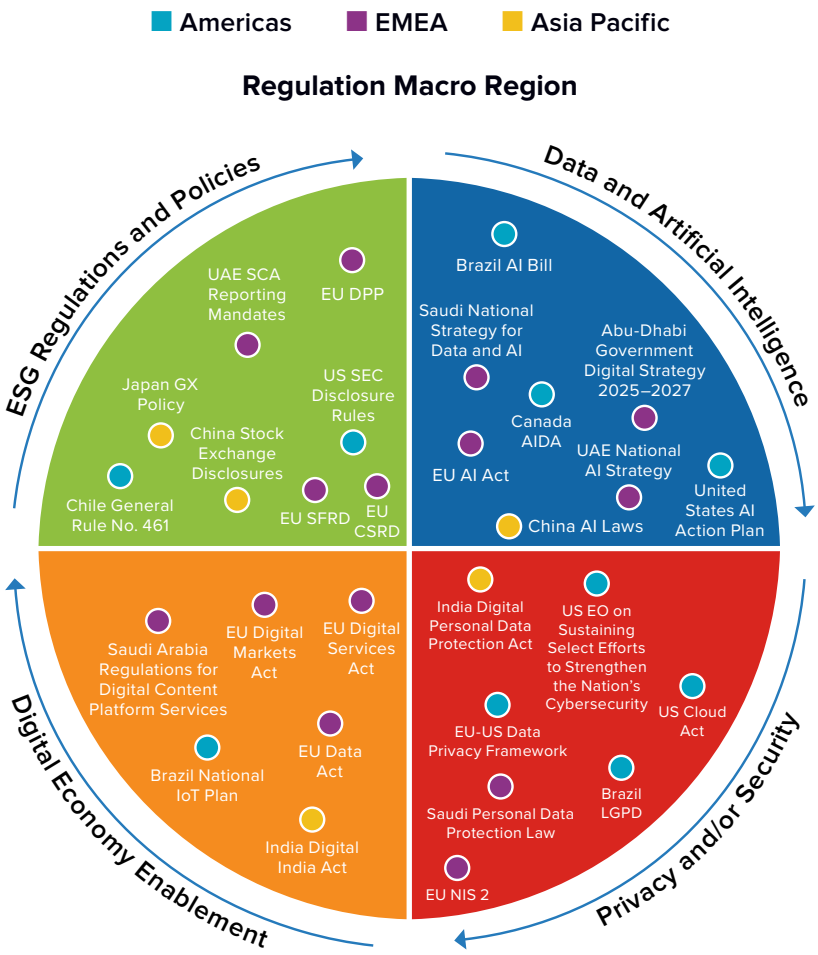
Source: IDC's *Worldwide Digital Sovereignty Survey, 2025*, July 2025, Europe (n = 955)

As discussed above, data sovereignty is typically instigated by the need for compliance with local rules and regulations, especially in jurisdictions where data protection authorities can levy harsh penalties on organisations that breach the rules and lose sensitive data as a result. Along with the high financial cost of these penalties, organisations face the prospect of reputational damage from which it could take years to recover. Data sovereignty is also triggered by concerns over extraterritorial jurisdictions requesting access to data when the data is archived by technology suppliers subject to those regulations – even when that data is archived in the country. The US Cloud Act epitomises this type of risk, even though it includes mechanisms for technology suppliers to lawfully challenge judicial orders, making its application extremely rare.

IDC tracks dozens of digital regulations and policies around the world. Figure 3 provides a snapshot of the most salient regulations that affect technology markets worldwide. The key areas of regulation are data and AI, privacy and security, digital economy enablement, and environmental, social, and governance (ESG).

FIGURE 3:

IDC's Worldwide Digital Regulations and Policies Radar



Source: *Worldwide Digital Regulations and Policies Radar, 2024* (IDC #US52354224, June 2024)

While these regulations do not specifically call for organisations to use sovereign solutions, some will stress the importance of data localisation and residency to help protect sensitive workloads against extraterritorial data requests. This, together with the overall need for compliance, prompts discussions about data sovereignty, especially for those organisations that are only just beginning their cloud journeys and are therefore factoring in all the things they will need to consider as part of their migrations.

Our 2025 survey reveals that the need to increase data privacy and security now ranks among the top three drivers (the need to enhance cybersecurity came in fourth last year). Here, it should be noted that sovereignty and security are not the same thing. While they can be considered two sides of the same coin, sovereignty is about control and transparency. An analogy to help illustrate this is to consider your car as your data. Once the car is locked, it can be considered secure. But who has access to the key? And can the car be used without your authority, and by whom? This analogy depicts the idea of control as the keystone for digital sovereignty.

While compliance is a key driver across all the regions included as part of IDC's latest digital survey, Europe is a significant exception. The year 2025 has introduced a dramatic change in market dynamics here. Our survey results reveal that the need to protect organisations against extraterritorial data requests is now the top driver on the continent (followed by the need to increase data privacy and security, and then the need for compliance with national/regional legislation). Europe can be regarded as the birthplace of digital sovereignty; calls in Europe for greater data protection and privacy have been the loudest over the years, especially due to concerns about the dominance of non-European technology providers. These concerns have been brought into sharper relief in 2025 due to geopolitical and economic uncertainties.

IDC research in recent years has consistently shown that, despite the anecdotal evidence and press attention it attracts, geopolitical uncertainty has typically been a low-ranking driver of organisations seeking digital sovereignty solutions. For example, in our *Worldwide Digital Sovereignty Survey, 2024*, geopolitical risks ranked at the bottom of the list of drivers, attracting just 20% of responses. But, in 2025, the need for protection against geopolitical risks has risen up the agenda, with a quarter of organisations surveyed citing this as a driver due to the economic and geopolitical turmoil witnessed since the beginning of the year.

Furthermore, when asked about the impact of geopolitical uncertainties so far seen in 2025, such as trade tensions, regional conflicts, or regulatory shifts, nearly half of organisations globally report increased interest in sovereign solutions since last year. The Middle East and Africa (MEA) and Asia-Pacific, including Japan (APJ), regions lead this trend, with over 50% of respondents indicating heightened interest. Europe, considered the vanguard digital sovereignty market, already had high interest in this area and started from a high base: 38% say their interest has remained the same, while 46% have increased interest. North America shows the highest decrease in interest (from what was already a minority).

This shift is not just about compliance. It reflects a broader recalibration of digital strategy, prioritising resilience, trust, and national interest due to rising cyberthreats, trade tensions, and AI-driven disruption. These are the chief dynamics that shaped global digital sovereignty developments and activities during the first half of 2025.

What Customers Need to Look For

Who Needs a Sovereign Cloud?

As has already been discussed, the key driver behind an organisation's decision to use sovereign cloud is to support requirements for regulatory and legal compliance, and these will vary depending on the rules that govern an individual industry sector and the digital laws that apply in the jurisdiction(s) in which it operates. Thus, the data that organisations need to consider for migrating to a sovereign cloud is primarily that subject to regulatory control, as not all workloads need to be moved to a sovereign cloud.

While this may suggest that the main industry users most likely to use digital sovereignty solutions are those in regulated sectors, this is not the case. In recent years, IDC research has revealed interest in digital sovereignty across all industries, albeit to varying degrees. When asked if they currently use sovereign public cloud solutions, 37% of organisations surveyed globally said they did. This was followed by 25% who plan to use such solutions in the next 12 months, and 19% who said they also planned usage, but not in the next 12 months. In terms of industries, the highest numbers of current users are in the telecoms, education, and business & personal services sectors; the top three industries that plan to use sovereign cloud solutions in the next 12 months are energy, telecoms, and manufacturing.

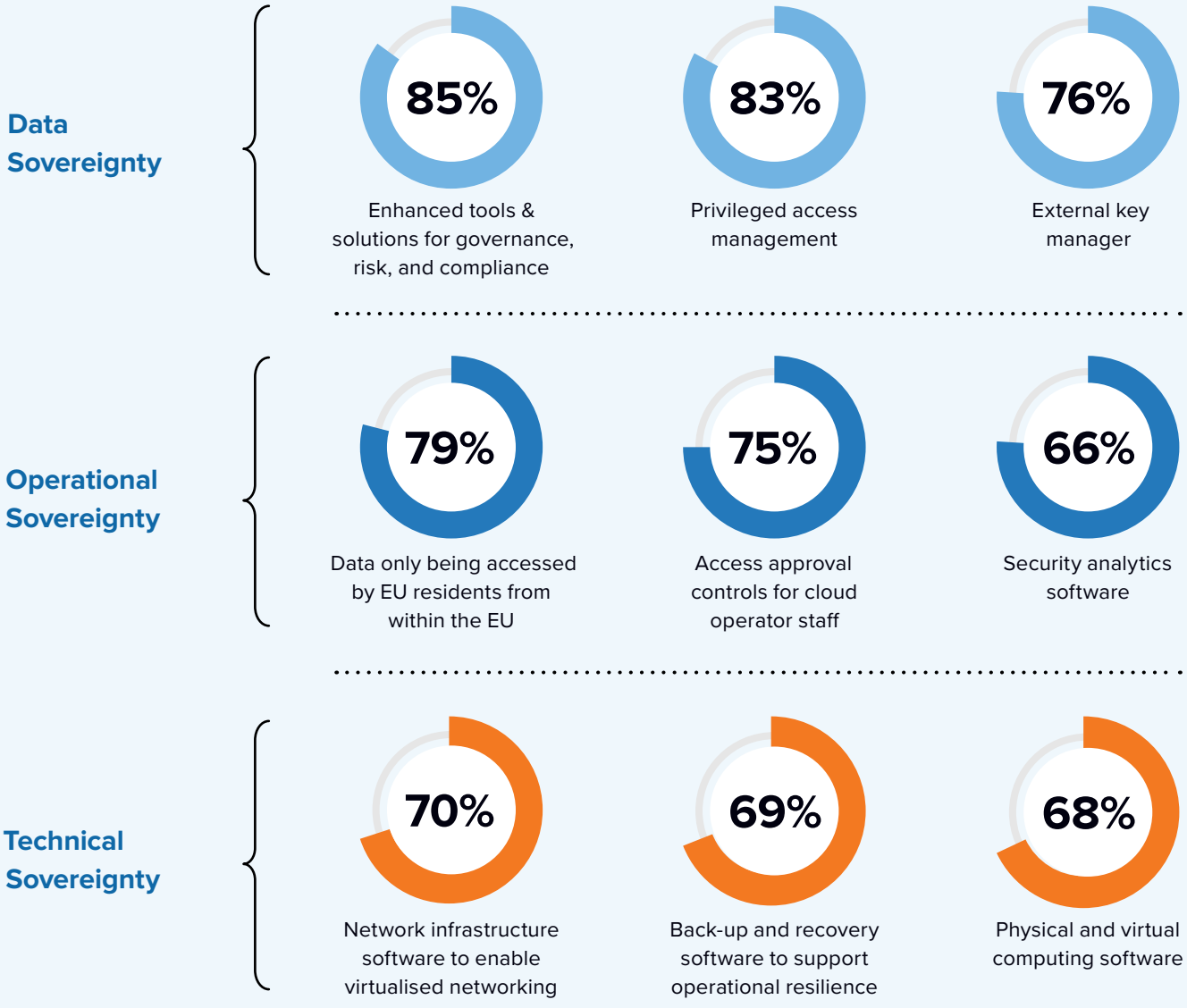
As well as the need for regulatory compliance, organisations should consider using sovereign cloud for any data that they classify with a high sensitivity rating – "top secret" or "highly confidential" workloads featuring data that, if leaked, would have catastrophic or serious business impacts.

Using Sovereign Cloud

As previously stated, IDC considers data sovereignty, technical sovereignty, and operational sovereignty as the three primary technology markets for building sovereign cloud. Figure 4 shows the top three rated IT and services that organisations consider to be either extremely important or very important for sovereign control in each of these markets.

FIGURE 4:

The Most Important IT Solutions and Services Needed to Support Data, Operational, and Technical Sovereignty



Source: IDC's *Worldwide Digital Sovereignty Survey, 2025*, July 2025, Europe (n = 955)

While the numbers shown here largely speak for themselves, two data points are worth highlighting.

Firstly, the top priority for 79% of organisations looking for solutions to support operational sovereignty is for their data only to be accessed by EU residents from within the EU. It would seem logical for readers to deduce that this response was mainly driven by the European sample from IDC's *Digital Sovereignty Survey, 2025*.

However, IDC's research was conducted worldwide, and this option attracted high responses (at least 78%) from across all the regions included in the survey. This illustrates that EU regulations are front and centre when it comes to driving digital sovereignty decisions, not only for European organisations, but for many enterprises doing business in EU member states. This also illustrates the underlying need for controls over identity and access management regarding sovereign cloud infrastructure, services, and platforms, as this is a key tenet of the overall concept of digital sovereignty.

Secondly, the dominant need for technical sovereignty is control over network infrastructure software to enable virtualised networking. This also includes related network infrastructure functions across enterprise, data centre, and communication service provider networks. Other network considerations for technical sovereignty include network management software for network performance and network operations. (This was chosen as the top response for this question by 53% globally.) Network sovereignty is crucial, as digital sovereignty means applying sovereign controls not only to data at rest but also to data in transit. Organisations looking to leverage digital sovereignty will therefore need to seek out network partners that have implemented sovereign controls across their network infrastructure and supporting services, such as network traffic monitoring and observability. This may prove challenging, as few telecom operators have considered this market niche; some are only now undergoing internal IT cloud migrations.

Many organisations will have varying requirements for digital sovereignty and may not need all the IT solutions that comprise each of the three technology areas described above. Identifying technology partners that offer the right-sized sovereign solutions that fit their individual needs is therefore crucial (see Choosing A Sovereign Cloud Partner).

Implementing Sovereign Cloud

IDC has developed the following **framework** to help organisations implement solutions for digital sovereignty:

- **Take stock.** One of the first steps for organisations is to review everything needed for digital sovereignty. This will include looking at skills for implementing, operating, and maintaining sovereignty, assessing the infrastructure and platforms required to support the implementation, and reviewing cybersecurity.
- **Determine your degree of data sensitivity.** This next phase is crucial and complex, as it requires organisations to classify their data according to sensitivity because not all workloads will need to be migrated to a sovereign cloud. Top secret or very confidential data should be classified with a high sensitivity rating. The leaking or compromising of this date will likely

have a catastrophic consequence on a business. More than a quarter of organisations globally say they have classified 41–50% of their data with a high or medium sensitivity rating.

- **Constantly monitor evolving regulatory landscapes.** Once solutions for digital sovereignty have been successfully deployed, organisations must ensure that sovereign controls are constantly maintained. They will need to keep an eye on the regulatory and legal regimes in which they operate to stay on the right side of data protection officers. This can be supported by dedicated APIs and AI.

- **Stay secure. Stay sovereign.** Cybersecurity should be a shared responsibility between the organisation and its sovereign services provider. In the case of a sovereign cloud, it is down to the user organisation to ensure that data remains protected across its operations, while the sovereign cloud provider must ensure the same across its sovereign infrastructure and software. Mutual trust is essential here, and organisations must seek out vendors that have all the credentials and expertise needed to maintain sovereign controls for cybersecurity (see Choosing a Sovereign Cloud Provider). All parties and their partners should ensure they remain sovereign today and tomorrow, which again emphasises the need to constantly monitor the regulations and legislation that apply to the relevant industry sector and market.

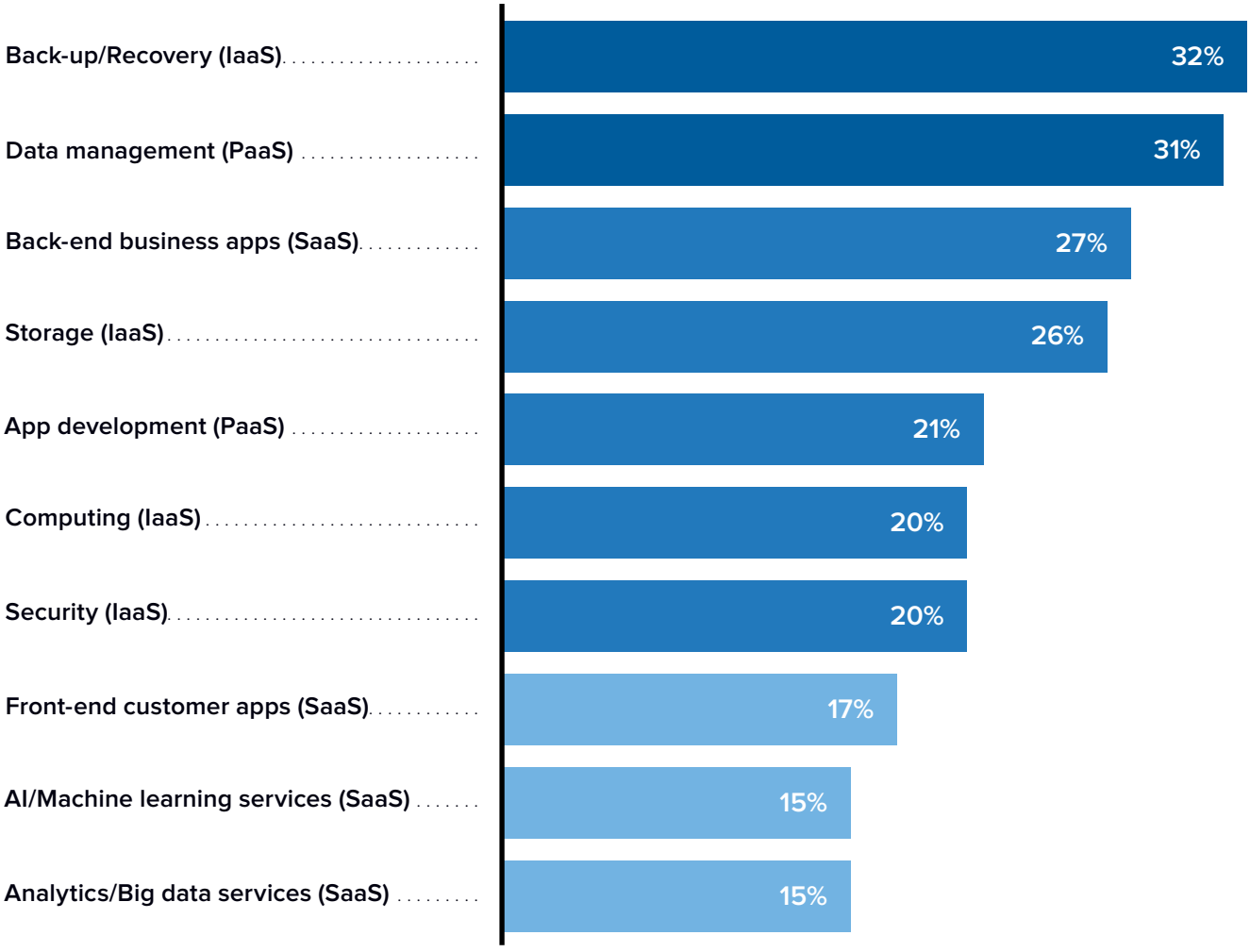
- **Scan the market to understand the evolution of sovereign cloud offerings.** Sovereign solutions are not limited to one archetype. They range from public cloud with sovereign controls and logically and physically separate computing environments dedicated to a country or an industry to managed sovereign clouds operated by global cloud and platform service providers partnering systems integrators or telecom service providers, and from solutions built, owned, and operated by cloud and platform services providers headquartered in the region or country to private cloud. These different archetypes have different costs, capabilities, and levels of control. Senior IT leaders must constantly engage with the market for advice on selecting the sovereign cloud archetypes and vendors that best fit their architectural roadmaps. (For a more detailed discussion, see Choosing a Sovereign Cloud Vendor).

Choosing Workloads to Migrate to a Sovereign Cloud

Once organisations have conducted reviews and classified their data as part of their preparations to implement a sovereign solution, they should identify the workloads most suitable for migration.

FIGURE 5:

Workloads That Organisations Have Either Migrated or Expect to Migrate to Sovereign Cloud



Source: IDC's *Worldwide Digital Sovereignty Survey, 2025*, July 2025, Europe (n = 955)

The top three workloads organisations are migrating, or are likely to migrate, to a sovereign cloud remain unchanged in 2025 from 2024 (IDC's *Worldwide Digital Sovereignty Survey, 2024*). However, data management has been pushed into second place this year, with back-up/recovery now occupying the top spot.

As explained earlier, organisations at all levels, including governments, must ensure their data is always available, and operational resilience is seen as one of the main business benefits of using sovereign cloud.

As seen in the results of last year's survey, AI/ML services feature at the bottom of the chart, with only 15% of respondent organisations globally saying this will be the workload they migrate/expect to migrate to a sovereign cloud. Many organisations will only use sovereign cloud for AI/ML workloads that are subject to regulatory compliance and/or require sovereign controls due to the high sensitivity of the data used, including those used for large language models (LLMs). However, geopolitical events have impacted AI deployment decisions, with 63% of the organisations stating in IDC's *Digital Sovereignty Survey* that national security and autonomy concerns, cross-border data access and surveillance, and regulatory uncertainty are influencing their interest in considering sovereign cloud for AI workloads. The next generation of GenAI and agentic AI workloads, which require large datasets for algorithm training and grounding, are driving senior IT leaders to seriously consider this deployment model.

AI is a double-edged sword in the sovereign cloud market. While sovereignty impacts AI workloads when they are subject to regulatory compliance and comprise high-sensitivity data, AI itself can also impact sovereignty. For instance, some providers have been showcasing solutions that could help organisations during the implementation and operational stages of a sovereign solution. These include tools to support sovereignty implementations with service control policies and non-compliance observability capabilities, AI security add-on features that enable IT teams to automatically classify and protect sensitive files, and AI functionality that enables users to ask about compliance issues in lengthy proposal documents.

How a Sovereign Cloud Fits into the IT Strategy

When organisations were asked where they primarily store data that they classify with high sensitivity ratings, the top answer for 29% of organisations globally is a public cloud from a local provider, followed by 23% that use a public cloud from a global provider.

Most organisations integrate a sovereign cloud into a hybrid IT environment, which is a combination of a public and dedicated (private) cloud, or as part of a multicloud approach. This should come as no surprise, as hybrid/multicloud IT has been the general trend in all cloud markets for several years now. More specifically, when asked how sovereign cloud fits into their cloud strategy, 55% of organisations indicated that a sovereign cloud will be part of their hybrid cloud/multicloud approach. However, what is more surprising is that 37% said they use on-premises IT and that a sovereign cloud is, or will be, the only type of cloud they use.

The industry sectors where this was selected as the highest positive response are healthcare (45%), manufacturing (42%), and retail (41%). When asked about the main reasons behind their decision to use sovereign cloud, aside from compliance, 37% of respondents in healthcare cited the need to increase customer trust, and 34% in manufacturing and 44% in retail (the top answer in this sector) stated the need to increase data privacy and security. These sectors have typically been relatively slow to adopt cloud computing services and technologies, and security and trust issues in the cloud remain top concerns as they progress along their digital migration journeys. As a result, organisations in these industries – alongside others with stringent compliance requirements or large numbers of organisations with highly sensitive data, such as government, education, and healthcare – are advised to seek solutions that offer greater control in technical sovereignty and operational sovereignty.

How Much for a Sovereign Cloud?

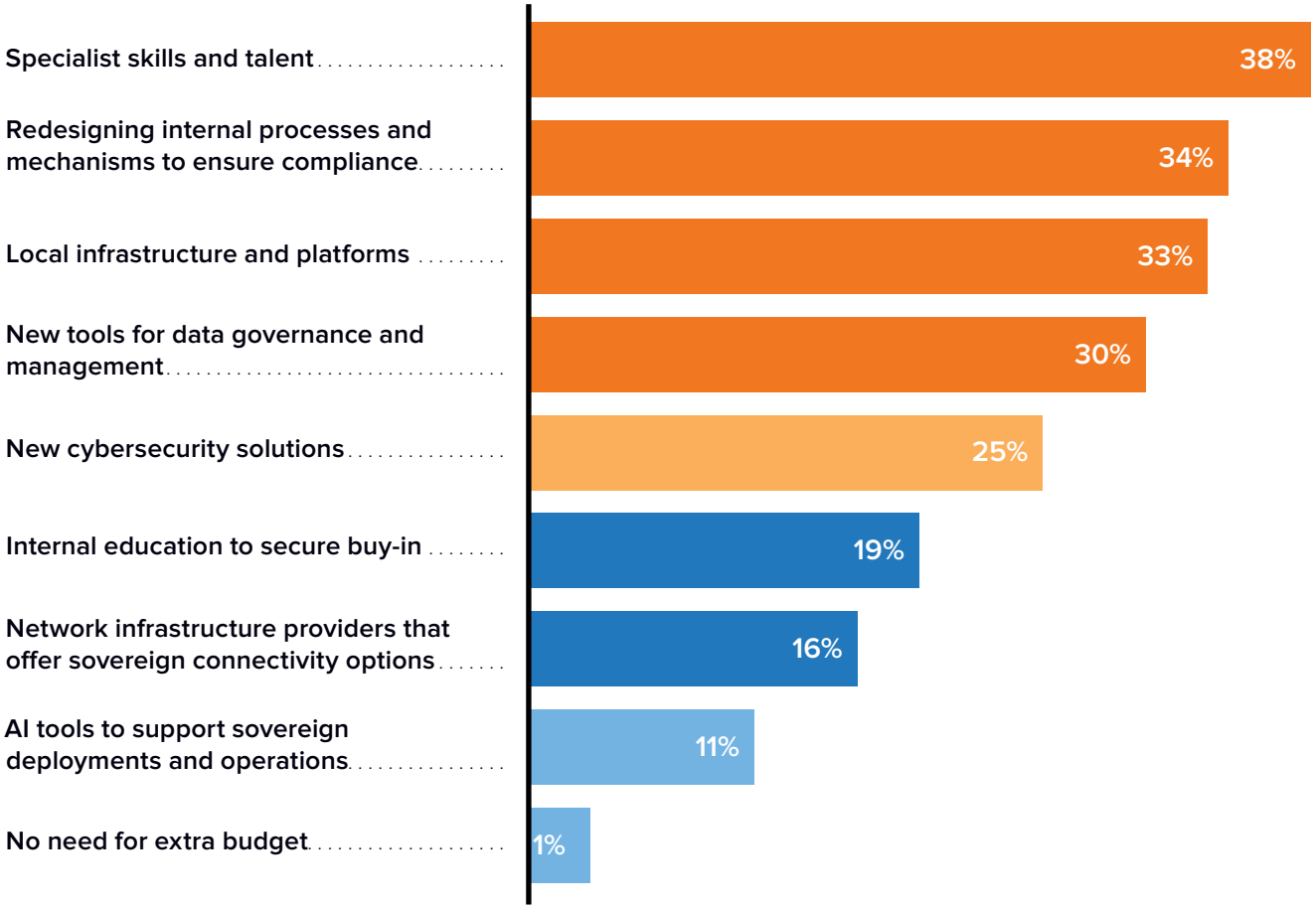
High cost remains one of the main challenges to be addressed when implementing digital sovereignty solutions (see Challenges for Users). Current economic uncertainties have clearly taken their toll on sovereign cloud budgets in 2025 because, when asked what percentage of their total public cloud spending is allocated to sovereign cloud solutions, the top answer for 35% worldwide is 6–10%. This is less than in 2024, when most organisations said they were willing to spend 11–20% of their existing IT budgets on a sovereign cloud solution. Despite growing demand for digital sovereignty, organisations are unwilling to pay high premiums for solutions. When asked how much they will be prepared to pay in 12 months, the numbers drop, with 31% willing to allocate 6–10% of their budget and another 30% only willing to invest 1–5%.

Furthermore, many organisations say they are unwilling to pay anything extra for individual solutions for data sovereignty, technical sovereignty, or especially operational sovereignty. In this regard, 23% in North America, 19% in MEA, 14% in APJ, and 14% in Europe believe solutions for operational sovereignty should be built into cloud offerings as standard and are thus unwilling to pay more for them.

As well as budgetary constraints, organisations face additional costs when implementing digital sovereignty solutions, as shown in Figure 6. Organisations must ensure they have all the skills needed to design, deploy, and operate sovereign architecture, and this is likely to require expertise not just in IT but also in matters of governance, compliance, and policymaking. Other likely investments include local infrastructure and platforms, new tools for data governance and management, and redesigning internal processes and mechanisms to ensure compliance.

FIGURE 6:

Areas Organisations Are Likely to Need Extra Budget When Implementing Data Sovereignty and Sovereign Cloud Solutions



Source: IDC's *Worldwide Digital Sovereignty Survey, 2025*, July 2025, Europe (n = 955)

Benefits of Digital Sovereignty

As with all enterprise digital initiatives, digital sovereignty solutions such as sovereign cloud should be regarded as a means to an end, and organisations should begin by considering the business outcomes they aim to achieve by implementing such solutions. Aside from the market drivers discussed above, sovereignty can potentially bring unique benefits to an organisation, including:

- **Greater data control:** Figure 2 shows that protection against extraterritorial requests ranks as the top sovereign cloud implementation driver for 32% of organisations globally. Accordingly, 35% of organisations globally agree that control of data transfers to protect the organisation against such requests is among the main benefits of sovereign cloud. Allied to this is data access control, which is another main advantage of using such solutions for 27% of our survey respondents. Greater data control can be further boosted by organisations partnering cloud providers with local data centres to support data residency and data localisation needs. This is seen as the top benefit of using sovereign cloud for 43% of organisations globally.

- **Becoming future-ready for digital regulations/legislation:** This readiness is particularly crucial in regions where the rules and laws governing enterprise IT use continue to evolve and change and new regulations are introduced. Europe provides an example. Since the introduction of GDPR in 2018, the EU has created many other regulations that apply to enterprise technologies. Along with the aforementioned Digital Operation Resilience Act, these include the Network and Information Security Directive, EU Cybersecurity Act, Digital Services Act, Digital Markets Act, and Chips Act. Ultimately, all organisations that use digital technologies and services need to keep a constant eye on what is required for sovereignty. While they may not necessarily need related solutions today, they may require them tomorrow.

- **An enhanced cybersecurity profile:** As already stated, sovereignty and security are not the same thing. However, many sovereign cloud offerings from major providers tend to have enhanced data security solutions – such as sophisticated encryption processes, confidential computing, and stringent guardrails – which has led to a market misconception that digital sovereignty equals cybersecurity. Some 41% of our survey respondents stated that enhanced data security and privacy is the top benefit of sovereign cloud for them.

- **Greater operational and business resilience:** This is regarded as the main benefit by 22% of organisations in Europe. Digital sovereignty solutions enhance operational resilience by giving organisations greater control over their data, infrastructure, and digital operations. By working with the right sovereign partners in their local jurisdictions, organisations can leverage sovereign solutions that reduce exposure to geopolitical risks, legal uncertainties, and global cyberthreats. This independence ensures that critical systems can continue functioning during disruptions – whether due to cyberattacks, outages, or regulatory conflicts – thereby strengthening business continuity and ensuring essential services remain available and secure under adverse conditions.

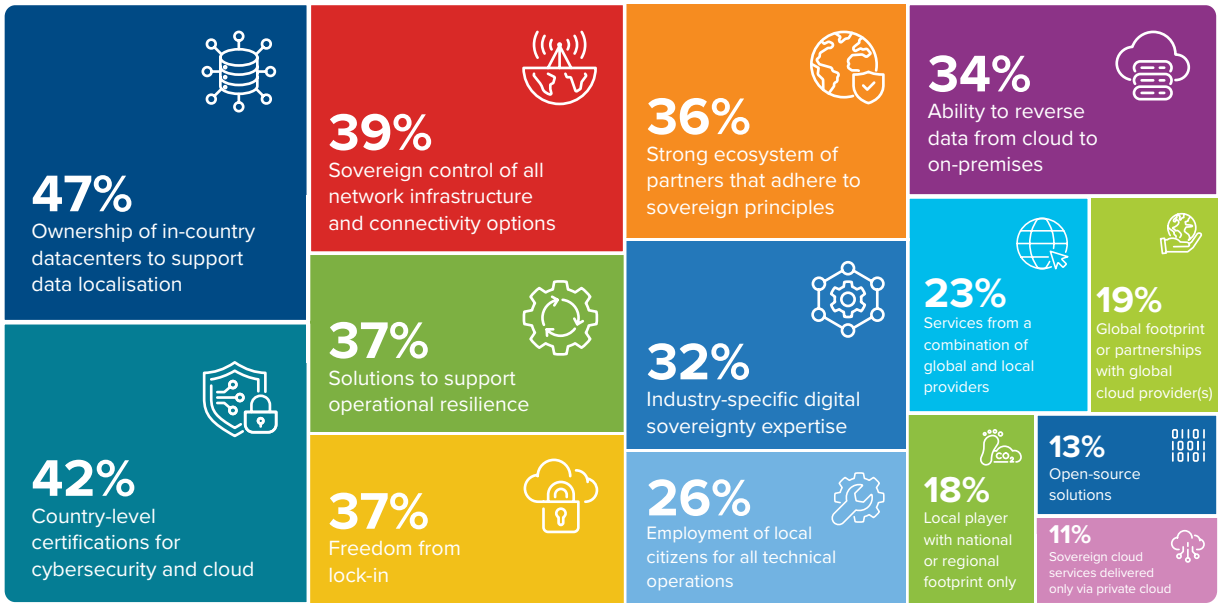
- **Gaining a competitive edge:** Far from being a necessary evil, digital sovereignty can give organisations a competitive edge, with 10% saying it can help open access to new markets. This is bolstered by greater customer and stakeholder trust, which is cited as a benefit by 15%. Trust is a highly sought-after attribute for customers and vendors alike, especially in the sovereign cloud market.

Choosing a Sovereign Cloud Partner

As mentioned above, organisations consider data residency and data localisation as the top benefits of using sovereign cloud. Therefore, the number one attribute they look for when selecting a sovereign cloud partner is ownership of in-country data centres to support data localisation. Some may disagree that actual ownership is not a vital part of sovereignty. It is certainly true that more emphasis should be placed on giving data owners complete control over their data and digital assets and protecting these against extraterritorial requests or any other unauthorised access. But those organisations that believe local data should be held on local soil by local providers also include ownership of the data centres in their quest for sovereignty. Thus, this is the top attribute sought when choosing a partner, as Figure 7 shows.

FIGURE 7:

What Organisations Seek When Choosing a Sovereign Cloud Partner or Provider



Source: IDC's *Worldwide Digital Sovereignty Survey, 2025*, July 2025, Europe (n = 955)

However, this does not mean that organisations only look for local players who only cover the national or regional market. Only 18% of organisations globally consider this to be a top priority. What is more coveted, at 36%, is a strong ecosystem of partners that adhere to sovereign principles. A trusted ecosystem of partners is needed for sovereignty to work at scale, and IDC believes this ecosystem should include a combination of global and local providers. For global cloud players, this means looking for the right regional and in-country partners to help boost local credibility, deliver local services and expertise, and leverage local knowledge. For the local service providers, this means partnering global players to help deliver innovation and scalability. Global SaaS providers, on the flip side, must be able to work across the board to develop and deliver customised offerings within sovereign frameworks.

Freedom from lock-in also ranks as a top attribute sought in a provider. It is important to consider digital sovereignty solutions that enable data portability, transferability, and interoperability. While this is especially true for corporations with a mixed IT estate and digital footprint that spans multiple jurisdictions, it applies to organisations with data subject to regulatory compliance, as they will need to use the right IT venue for the right workload. That means working with a provider that offers the flexibility to do so without fear of lock-in or egress charges, for example.

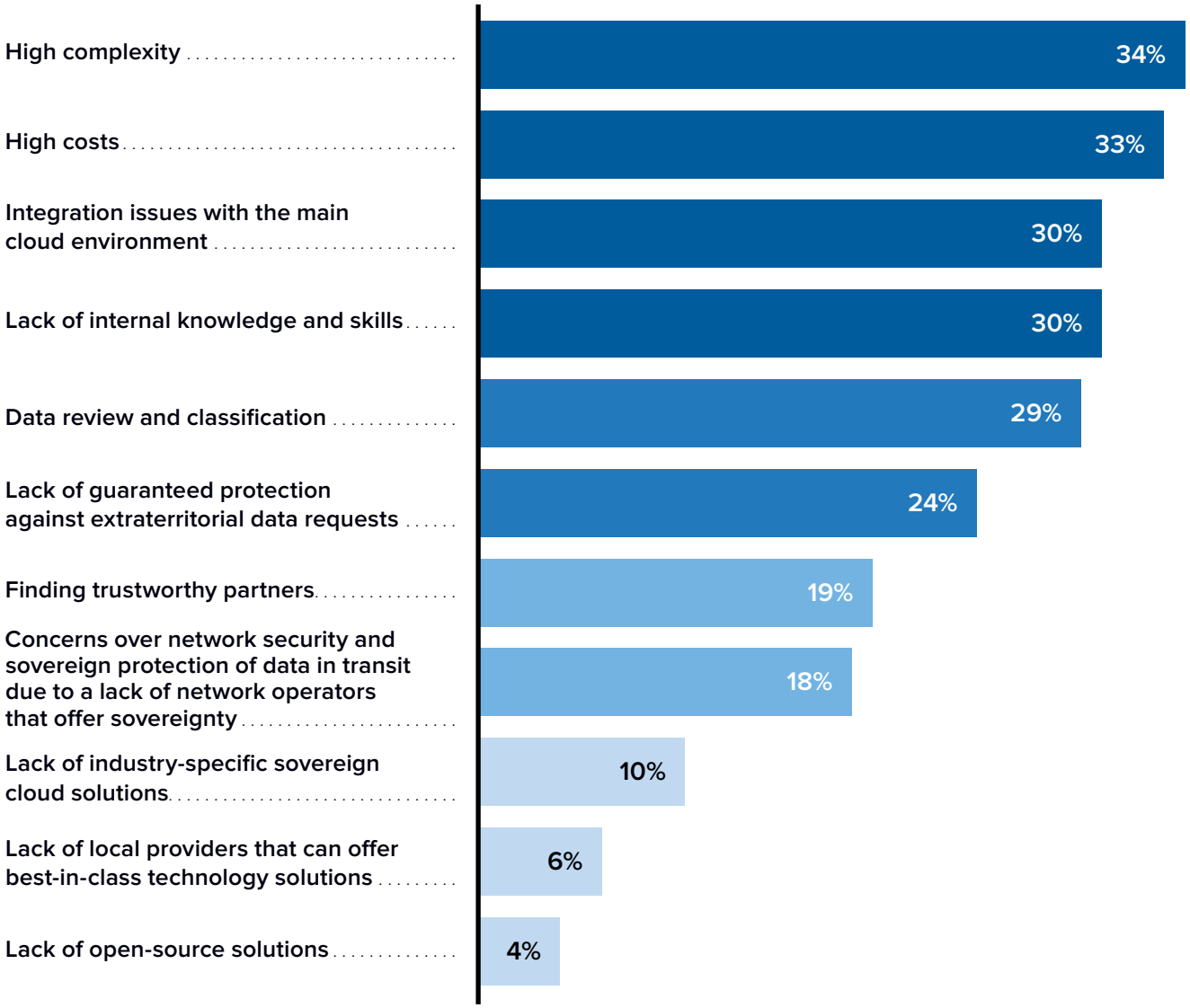
Open-source solutions (which are important for 13%) can also help avoid vendor lock-in, although the trade-off to consider here is the innovation quality of open-source solutions compared with proprietary and closed-source offerings. Sovereignty solutions can, by their very nature, be restrictive, so organisations must ensure that they balance the need for sovereignty with their need for innovation.

Challenges for Users

High complexity and high costs have consistently ranked in our surveys in recent years as the two main challenges organisations face when implementing a sovereign cloud.

FIGURE 8:

The Main Challenges for Organisations in Implementing Sovereign Cloud



Source: IDC's *Worldwide Digital Sovereignty Survey, 2025*, July 2025, Europe (n = 955)

Complexity begins from the outset of the sovereign cloud journey, when users need to classify their data and workloads according to sovereign requirements and then review what they will need to meet those requirements. This is highlighted in Figure 8, which shows that reviewing and classifying data is the top obstacle

for 29% of organisations worldwide. The complexity is greater when integrating a sovereign cloud into an existing IT environment, especially when that environment comprises a mixed estate. Integration issues are a hindering factor for 30%. And, if all that was not enough, all these complexities are exacerbated throughout the lifetime of a sovereign cloud. Organisations will need to constantly monitor their entire ecosystems of sovereign solution partners and providers to ensure that sovereign controls and compliance are maintained over the long term and in changing regulatory environments (and across multiple jurisdictions, in the case of organisations with multinational digital footprints).

High costs have also been consistently identified as a top challenge to sovereign cloud use. Extra costs can include investments in local infrastructure and platforms, new tools for data governance and management, and expenditure on redesigning internal processes and mechanisms to ensure compliance.

For most organisations, specialist skills will be needed to implement and operate a sovereign cloud environment, which may require further investments in training or hiring new talent, thus adding to already-high costs. Aside from overall cloud and security know-how, organisations will need technical specialists with expertise in data management and governance and some degree of jurisprudence. More specifically, when asked in which areas they need additional skills and training to address emerging digital sovereignty requirements, the top five answers for organisations are data management & data analytics (52%), cybersecurity (46%), data classification (45%), governance (45%), and CloudOps (40%) (source: IDC's *Worldwide Digital Sovereignty Survey, 2024,* June 2024, N = 675).

To help overcome the obstacles, customers will need to work with trusted partners that can support them in assessing and defining the scope of a sovereign cloud strategy and help them win additional budgets and corporate mindshare. It is worth reiterating that trust is a vital tenet of digital sovereignty. It should be borne in mind that trust is not only applicable to the main sovereign cloud vendor but also to its entire ecosystem of supporting partners and providers. This demands a high degree of transparency on the part of the partner and is a challenge for almost a fifth of organisations, for which finding trustworthy partners is their greatest hurdle.

Who Should Be Involved in Digital Sovereignty Discussions?

Of the 955 respondents polled in IDC's *Digital Sovereignty Survey, 2025*, 56% are in IT/data roles within their organisations and 44% are from lines of business.

When asked about their role regarding decisions related to their organisations' digital sovereignty solutions, those in business roles emerged as the primary decision makers (32%), while those in IT had the most influence (47%). While IT and business departments are both part of the overall decision-making team, those from the latter dominate (41%).

All the above means that a cross-section of stakeholders from all lines of business within an organisation should discuss digital sovereignty requirements and solutions from the outset, as should be the case with all digital initiatives. While we often hear the refrain, "IT should talk the language of business," for successful implementations and operations, business should also talk the language of IT. At the very least, both should have meaningful discussions about how business outcomes and IT requirements impact one another.

Choosing a Sovereign Cloud Solution

Most of the major global cloud players now offer sovereign cloud solutions. These broadly fall into two categories. First are those "designed for sovereignty," which include offerings purpose-built for the sovereign cloud market and branded as such. The second category is "sovereign by design." Vendors that offer the latter solutions claim they have been developed with sovereign controls already built in from the outset or can have such controls retrofitted to existing products.

More recently, some vendors believe sovereign cloud is more optimally delivered via the private clouds offered by partners. While sovereign partnerships are laudable, IDC's latest research shows that only 11% of organisations around the world look for sovereign cloud services delivered exclusively via private cloud (see Figure 7).

The ideal solutions offer a variety of sovereign platforms and services tailored to an individual organisation's needs. These can vary from small-scale solutions, mainly to support data sovereignty requirements, to full-blown offerings that encompass controls for technical and operational sovereignty. For those with the highest sensitivity workloads and top-secret data – military or government organisations, for example – an air-gapped cloud that is completely disconnected from public cloud and disconnected from the internet would be the top consideration.

What should be clear here is that one size does not fit all industries in all markets. It is therefore crucial to work with sovereign cloud partners and providers that offer:

- Expertise and an understanding of what specific industry users need to develop customised sovereign solutions
- Flexibility to support data portability and to avoid vendor lock-in
- An ecosystem of specialists that can guarantee sovereignty to support the customer's various IT requirements
- Transparent guarantees to safeguard cybersecurity and data controls.

Advice for IT Decision-Makers and CXOs

- Not all workloads need to be migrated to a sovereign cloud. Organisations should begin by reviewing all their IT and associated needs for sovereignty. They should then classify their workloads according to compliance requirements as determined by their industry's regulations and local jurisdictions. They should also classify their data based on sensitivity and consider these workloads first for moving to a sovereign cloud.
- Organisations must be prepared to address challenges such as high complexity, high costs, and a lack of skills and knowledge. Further complexities include integrating a sovereign cloud into different IT environments, such as multicloud or hybrid estates. Organisations should look for trustworthy expert partners and providers that can be relied upon to help overcome these obstacles.
- Digital sovereignty will require additional investments in new tools for data governance and management, the redesign of internal processes to ensure compliance, and new skills to support the sovereign cloud environment. New infrastructure and platforms will also be needed.
- Maintaining and monitoring cybersecurity and regulatory compliance is vital and must be ongoing. Crucially, this responsibility must be shared among all partners. Customers and their partner providers must work collaboratively throughout the entire process of deploying and operating a sovereign solution.
- Partnerships with global and local providers are vital for sovereignty to work at scale, as well as to help maintain a balance between an organisation's need for sovereignty and its desire to harness cloud's innovation potential.
- Some 18% of organisations have concerns about network security and the protection of data in transit due to a lack of network operators that offer sovereignty. Beyond applying sovereign controls to data at rest, doing the same for data on the move as it traverses networks adds further complications, given the different network technology and operator types involved in cross-border data flows. Data on the move across networks presents a potentially bigger attack surface, necessitating sovereign control of all network resources. Organisations should therefore seek network partners that can guarantee such controls.
- Solutions that lead to vendor lock-in will restrict customers' data manoeuvrability. Open-source solutions lend themselves well to data interoperability, portability, and transferability, which is key to sovereignty success.

Advice for Policymakers

Policymakers should consider digital sovereignty as a continuum of options, whereby they can mandate stricter or more relaxed rules depending on the benefits they want to achieve and the related risks. On one end of the spectrum, policymakers who embrace a free-market scenario will ensure strong competition among all international IT suppliers, thus driving down prices and expanding the products and services available, but will expose their markets to higher compliance and security risks. At the other end of the spectrum, policymakers that isolate their digital economies by imposing autarchic sovereign requirements will increase the risk of being left behind in terms of innovation and will have to make direct government investments in skills that cannot be supplemented by international knowledge transfer; furthermore, they will decrease the resilience of national critical digital infrastructure because such countries will have no fallback alternatives.

Ministers, secretaries, and commissioners who want a balanced approach between the fast-paced innovation and resilience of open markets and the need to self-determine the destiny of their country's digital economy should:

- Map the external risks, starting with geopolitical volatility, intended economic competitiveness, and national security goals. A thorough and dynamic analysis will enable them to define potential scenarios that inform policy choices.
- Investigate the digital sovereignty regulatory landscapes that other countries are implementing to look for lessons learned. Start with the European Union and European Union member states, where the digital sovereignty initiatives are more advanced, but also consider emerging countries such as Saudi Arabia and the UAE. Do not limit regulatory analysis to data protection and cybersecurity regulations; consider the broader scope of AI strategies and action plans, energy resilience, sustainability strategies, intellectual property regulations, and public procurement regulations.
- Consider the interdependencies of all the attributes of digital sovereignty – from data, technical, operational, and assurance requirements to supply chains and geopolitics – to ensure regulations are effective. As AI takes centrestage, consider the sovereignty attributes of the whole AI ecosystem, from infrastructure and data to models and applications.
- Invest in literacy and talent development. Rapid innovation in areas such as cloud,AI, and cybersecurity impacts the ability of private and public sector organisations to make strategic and operational digital sovereignty decisions. Policymakers play a pivotal role in providing funding programs and creating public-private-academic collaborations that can accelerate talent generation for those areas.
- Activate forums and committees to help other policymakers, private sector CIOs/CTOs/CAIOs, academic experts, and technology suppliers understand the impacts of digital sovereignty regulatory interventions on both IT demand and IT supply.

CASE STUDIES:

Case Study

A European telecom operator needed to modernise a 20-year-old data ecosystem of over 40 legacy systems holding sensitive data, subject to European regulations such as the GDPR and national data protection regulations. The telecom operator built a cloud-native one data ecosystem (ODE), leveraging Google Cloud's sovereign cloud offerings, including a data boundary provided by a national systems integrator and External Key Management (EKM). This architecture allows the telecom operator to retain full cryptographic control over its data, with encryption keys managed entirely outside Google's infrastructure.

With this sovereign cloud architecture, the customer achieved:

- Full data sovereignty: protects sensitive data from foreign legal frameworks
- Cloud-native innovation: enables secure in-cloud processing of sensitive data
- Regulatory compliance: meets stringent European data protection laws
- Operational efficiency: consolidates fragmented systems into a unified and scalable platform

Case Study

A provider of regulatory reporting solutions for finance institutions and regulators needed to handle sensitive financial data across jurisdictions while ensuring compliance with regulations like the GDPR and DORA.

This customer built a cloud-native platform using Google Cloud's confidential computing, sovereign controls, and EKM, ensuring:

- Improved data security and compliance: data encrypted and under customer control at all times
- Enhanced scalability and performance: handling large volumes of regulatory data
- Greater flexibility: offering more agile and secure services that meet finance institutions' and regulators' needs

Research Methodology

Most of the data used in this IDC White Paper is from IDC's *Worldwide Digital Sovereignty Survey, 2025*, conducted in May and June 2025.

The survey questioned 955 organisations with 500+ employees operating in the following industries: construction, education, energy, finance, government, healthcare, life sciences, manufacturing, professional services, retail, telecom & media, and transport & logistics. All the organisations included are currently using or planning to use cloud computing services and technologies and are currently using or planning to use sovereign cloud.

The research was conducted using computer-assisted telephone interviewing (CATI) across a global sample. This included 410 respondents from Europe, 255 from AP (including Japan), 150 from North America (the USA and Canada), and 125 from MEA (including Turkey).

The target respondents included a mix of IT (professional level and above) and line-of-business (manager and above) employees responsible for influencing their organisation's sovereign solution strategy.

The purpose of the survey was to uncover the business potential for digital sovereignty, including market drivers, spending expectations, challenges, and the building blocks users will implement over time.

The study broadly reinforces and adds to IDC's insights, forecasts, and analytical expertise about the growing importance of sovereign cloud. It also assesses market understanding of sovereign cloud to support IDC's taxonomy and definitions of sovereign cloud.

Further Reading

- *How to Deal with the Shortage of Skills Needed for Digital Sovereignty* (IDC #US51630024, Mar 2025)
- *What Do Organizations Look for When Choosing a Sovereign Cloud Provider?* (IDC #US52595924, Sep 2024)
- *IDC's Worldwide Sovereign Cloud Taxonomy, 2024* (IDC #US50699324, Sep 2024)
- *An Assessment of Sovereign Cloud Solutions Offered by Five Global Cloud Providers* (IDC #EUR151605024, Jan 2024)

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 the IDC Analysts

Rahiel Nasir

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

Rahiel Nasir is responsible for leading and contributing to IDC's European Cloud and Cloud Data Management research programs, as well as supporting associated consulting projects. In addition, Rahiel leads IDC's Worldwide Digital Sovereignty research program. He has been monitoring technology markets and writing about them throughout his professional life. Prior to joining IDC, Rahiel was a research analyst with 451 Research (now part of S&P Global Market Intelligence), where he covered the data centre infrastructure and services markets across the EMEA region.

More about Rahiel Nasir

Massimiliano Claps

Research Director, IDC Government Insights

Massimiliano (Max) Claps is a research director in the European IDC Government Insights team. Max's research empowers technology suppliers and public sector professionals to embrace disruptive technologies such as artificial intelligence, edge computing, and cloud to realise the benefits of strategic initiatives such as smart cities and citizen-centric government services. Max is also IDC Europe's lead analyst for passenger transportation, advising stakeholders across the transportation ecosystem on topics like mobility as a service and intelligent traffic management. In addition to his public sector expertise, Max Claps also co-leads IDC's Europe, Middle East and Africa Cross-Industry Strategies and Use Cases thought leadership research.

More about Massimiliano Claps

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, IT benchmarking and sourcing, 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. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.)

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, 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 UK
1st floor, Whitfield Street, London, W1T 2RE, United Kingdom
T 44.208.987.7100

@idc | @idc | idc.com