White Paper

Cloud Sovereignty: A Strategic Imperative for Businesses in the Digital Age

Sponsored by: Tata Consultancy Services and HPE

Rahiel Nasir
April 2026

IN THIS WHITE PAPER

CXOs and their executive teams are seeking IT solutions that strengthen their organizations' strategic roadmap, addressing regulatory complexity, data privacy, operational resilience, and the imperative to innovate in an increasingly uncertain geopolitical landscape. As sovereign cloud becomes a strategic imperative for meeting evolving demands and maintaining control over an organization's digital assets, there is a clear need to demystify its concepts and practical implications.

This white paper clarifies digital sovereignty and its subsets, including sovereign cloud and sovereign AI, and examines the current landscape, what's driving the market, and what CXOs need to look for when choosing and implementing digital sovereignty solutions.

Unless otherwise indicated, the figures and data used in this report are taken from IDC Europe's Worldwide Digital Sovereignty Survey, 2025.

THE CIO AGENDA: WHY CLOUD SOVEREIGNTY? WHY NOW?

Compliance is the primary driver for the majority of organizations worldwide seeking sovereign cloud solutions. When asked what was behind their decision to use sovereign cloud, the top 3 responses selected included compliance with national/regional legislation (37%), the need to increase data privacy and security (35%), and compliance with industry regulations (34%). All of these are crucial in jurisdictions that have data privacy laws policed by data protection authorities that can levy harsh penalties on organizations that breach the rules and lose sensitive data as a result.

Along with the high financial cost of these penalties, organizations face the prospect of reputational damage from which recovery would take years. Failure to comply can result in severe financial penalties and reputational damage.

April 2026, IDC #AP15044X-P

Given these pressures, understanding the concept of digital sovereignty is essential for organizations evaluating their cloud strategies.

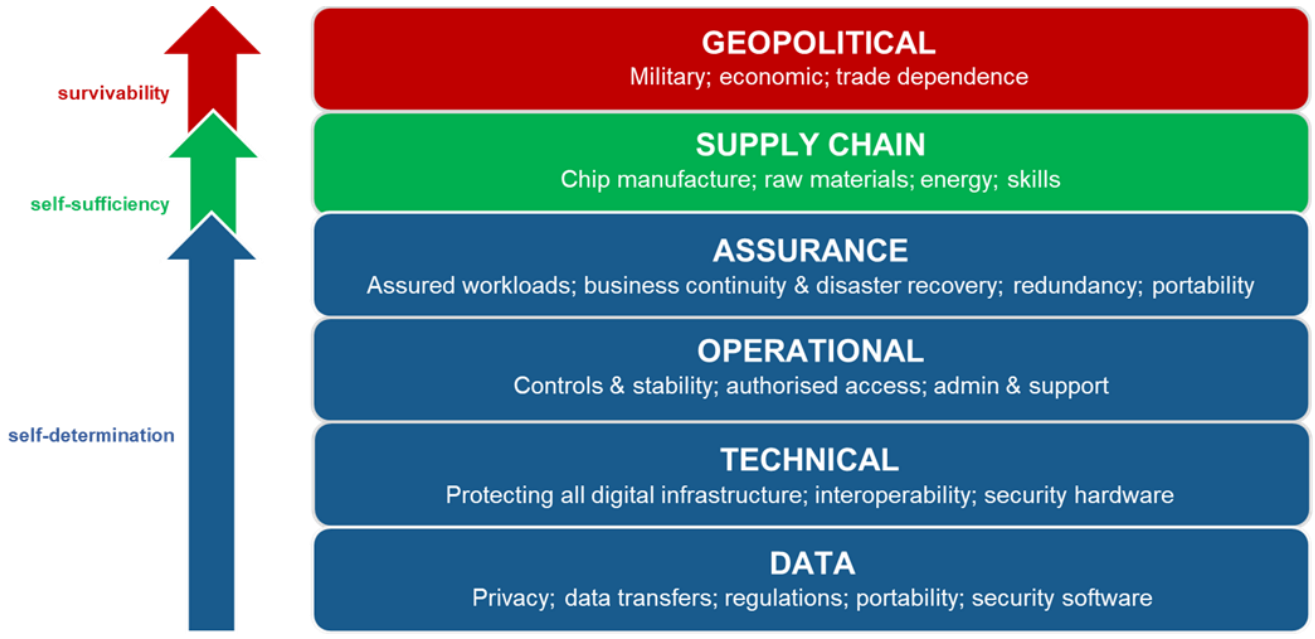
Defining Digital Sovereignty

IDC formally defines digital sovereignty as the capacity for “digital self-determination by nations, organizations, and 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. This includes all underlying infrastructure used for the data, such as datacenters and networks, as well as the support and admin staff who have access to that data and infrastructure.

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

FIGURE 1

The Various Attributes of Digital Sovereignty - IDC's "Digital Sovereignty Stack"



Source: IDC's Worldwide Sovereign Cloud Taxonomy, 2024

IDC considers data sovereignty to be a subset of the overall concept of digital sovereignty. Personal data privacy laws, such as the General Data Protection Regulation enacted across

the European Union in 2018, India's Digital Personal Data Protection Act that came into effect in 2023, Saudi Arabia's Personal Data Protection Law that became fully enforced since 2024, among others, typically kickstart the journey towards digital sovereignty. This requires solutions for data sovereignty. Here, organizations look for IT technologies and services that provide a holistic view of how data are collected, classified, processed and stored, and then managed and monitored to ensure that regulatory compliance is always being met.

Cloud sovereignty

Sovereign cloud can be regarded as another subset. As the foundation for digital business innovation, cloud will be at the core of digital sovereignty developments. The concept of cloud sovereignty (or sovereign cloud) encompasses IT services and solutions that fall under three primary categories:

- **Data sovereignty:** This includes solutions that provide a holistic view of how data is collected, classified, processed, and stored to ensure that data legislation and rules are being met. This requires the constant monitoring of how digital regulations and laws continue to evolve.
- **Technical sovereignty:** This refers to digital infrastructure located in a sovereign environment. This includes the datacenters plus all the servers, IT hardware, software, and XaaS used for cloud-based data and workloads. All this infrastructure should be shielded from non-sovereign digital infrastructure, as well as protected from all extra-territorial interference and scrutiny.
- **Operational sovereignty:** This includes solutions that offer cloud capabilities that enable transparency in controlling operations, from provisioning and performance management to the monitoring of physical and digital access to the infrastructure.

AI sovereignty

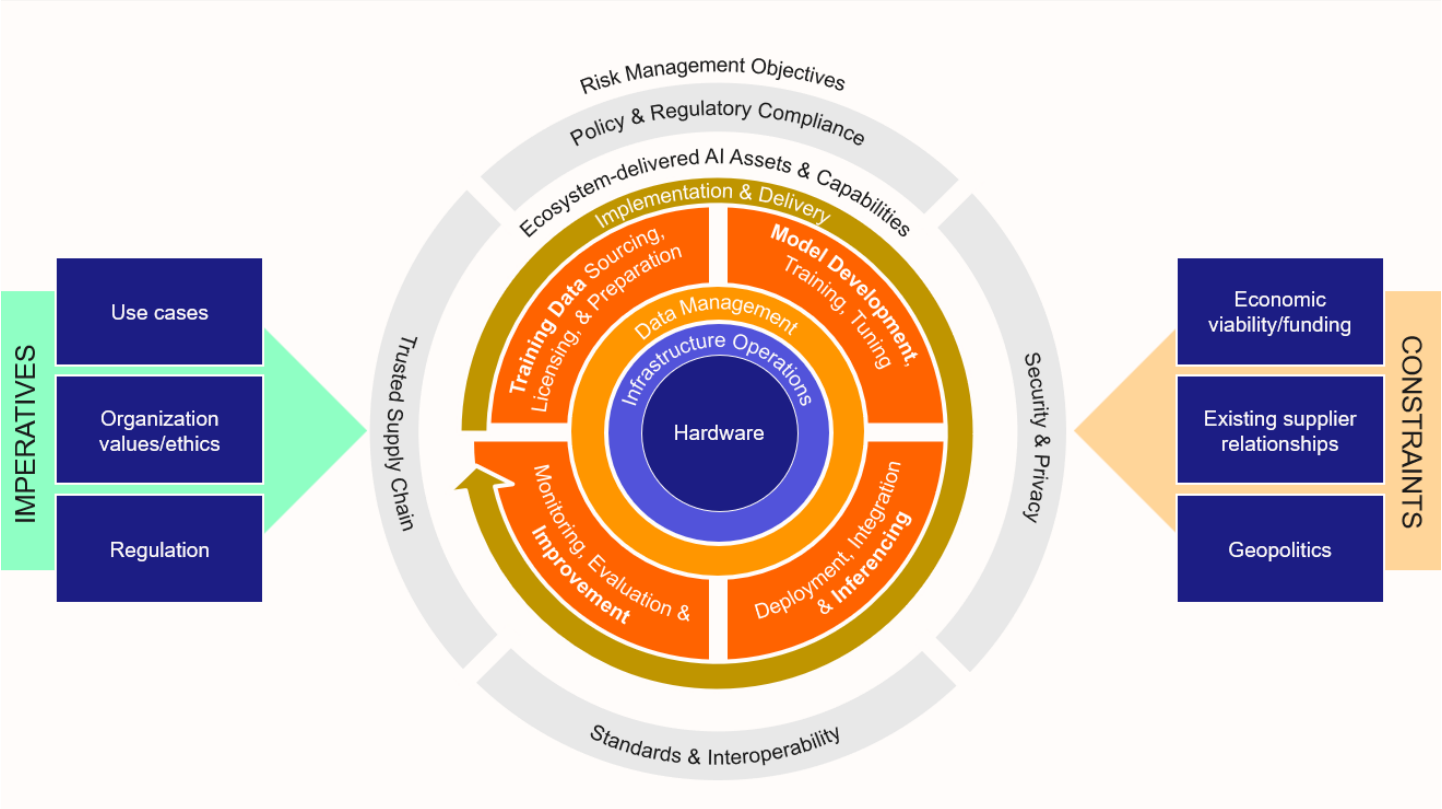
More recently, a third subset of digital sovereignty has emerged: AI sovereignty. India's AI Strategy (2024-2026), Saudi Arabia's National Strategy for Data & AI, the Abu-Dhabi Government Digital Strategy 2025-2027, and the European Union's AI Continent Action Plan are just some examples of how policymakers around the world have earmarked AI as a strategic lever to achieve economic competitiveness and digital leadership, as well as national security strategic goals. Achieving all this requires the application of sovereign controls across all the end-to-end AI stack, as shown in Figure 1, and beyond. That includes the ability to safeguard supply chain sovereignty for crucial resources such as GPUs, chips, AI models and talent.

AI sovereignty is a dimension of an AI strategy that describes the ability to have free choice and control over the design, development, deployment, accessibility, operation,

maintenance and governance of AI systems and applications, and the technologies that those systems and applications depend on.

FIGURE 2

IDC's Sovereign AI Framework



Source: Sovereign AI: What, Why and How, November 2025

IDC's Sovereign AI framework focuses on the levers that organizations can use to exert more control and choice over all facets of AI implementations and their underlying technology foundations.

The core of the framework comprises the assets and capabilities required to deliver a working AI system that delivers business value:

- At the center is the hardware and connectivity infrastructure as well as the hosting services that bring that infrastructure to life.
- Data management is the next layer. Here, organizations are concerned with where and how data is stored, as well as who has access to it.

- Around the data management layer is a set of capabilities required for the full AI system life cycle: from sourcing high-quality training data to training and tuning models, deployment and inferencing, and improvement.
- At the edge are capabilities related to implementation and delivery. These may be brought to life through internal staff resources, external service providers, or a mix.
- Around the edge of the framework are four risk management objectives that commonly shape interest in sovereign AI. These objectives will matter to different extents to different organizations and in different situations.

On the left of Figure 2 is the set of imperatives that are driving interest in sovereign AI:

- Regulation often dictates certain approaches. Most relevant regulations currently focus on constraining how data can be stored, managed, and accessed; under which conditions; and for which purposes.
- An organization may also have specific values or ethical approaches that shape how it thinks about control, choice, and independence.
- Lastly, individual use cases shape the need for sovereignty. Some use cases (for example, using generative AI or GenAI to create a marketing plan outline or a simple illustration for a marketing campaign) may not introduce significant requirements for sovereignty.

On the right of Figure 2 is a set of constraints that will also determine an organization's response to AI sovereignty concerns:

- Geopolitical factors may mean that some technology ecosystem players, or vendors from one territory or other, are prioritized over others.
- Existing supplier relationships may mean that some control options are "off the table".
- Some desired sovereign AI "levers" may, in practice, incur too much cost to be justifiable for some organizations or AI use cases.

Using Sovereign Cloud for AI Workloads

Demand for AI sovereignty does not necessarily (or solely) translate directly into demand for sovereign cloud; sovereign clouds are but one control lever clearly aligned with the hosting and hardware elements of IDC's Sovereign AI framework. However, it has become clear that organizations see a strong association between AI sovereignty and sovereign cloud.

IDC research indicates that global sovereign cloud usage for AI will accelerate in the next two years, with 48% of organizations planning to increase spending. This expansion reflects the alignment of multiple drivers: regulation, risk management, and national strategies.

Compliance is the primary driver for organizations to increase their use of sovereign cloud for AI. This reflects the widening scope of regulatory frameworks and the operational need to remain compliant across multiple jurisdictions. Rather than being just a box-ticking exercise, compliance now functions as a strategic capability. Many organizations want to be ready in terms of compliance to deploy AI across multiple markets without re-engineering their architectures. This approach may support business continuity amid changing laws, data transfer restrictions, or geopolitical uncertainty.

Closely following compliance is the desire for greater control over AI model governance and transparency. Organizations increasingly view sovereignty as a foundation for responsible AI. Therefore, ensuring visibility into how models are trained, what data they use, and how outputs are managed is becoming essential.

Concerns over vendor lock-in and extraterritorial data access further reinforce enterprises' desire to seek autonomy. European and MEA organizations express caution toward dependency on global providers. Organizations in these regions are showing a preference for hybrid cloud and multicloud approaches that ensure stricter local control and flexibility in compliance.

2025 was characterized by geopolitical turbulence, and this turned digital sovereignty into a form of strategic insurance. Events such trade tensions, regional conflicts, and shifts in data localization laws are a stark reminder to organizations that access to digital infrastructure can be disrupted overnight. For 63% of organizations worldwide, geopolitical tensions have heightened enterprises' interest in using sovereign cloud for their AI workloads. Their motivation is not only defensive; those seeking sovereign solutions also want bargaining power when negotiating with providers.

REGIONAL MARKET DYNAMICS

Europe: The Birthplace of Digital Sovereignty

A combined 60% of organizations in Europe are either currently using sovereign cloud solutions or plan to do so in the next 12 months. A further 22% say they plan to use such solutions sometime after the next 12 months. On top of all that, 46% in Europe say that compared to 2024, their interest in implementing digital sovereignty solutions has increased due to the all the geopolitical uncertainties seen in 2025. As a result, while compliance continues to be a key driver, the need to protect against extra-territorial data requests is of greater significance in Europe where this now the top sovereign cloud market driver. Many organizations in the region have heightened concerns over extra-territorial jurisdictions requesting access to data held by technology suppliers subject to regulations such as the U.S. Clarifying Lawful Overseas Use of Data Act (CLOUD) Act. This 2018 U.S. law is

usually cited as epitomizing this type of risk, even though U.S. technology suppliers can lawfully challenge any judicial orders invoked as part of the Act.

Middle East & Africa (MEA): Sovereignty as a Pillar of National Strategy

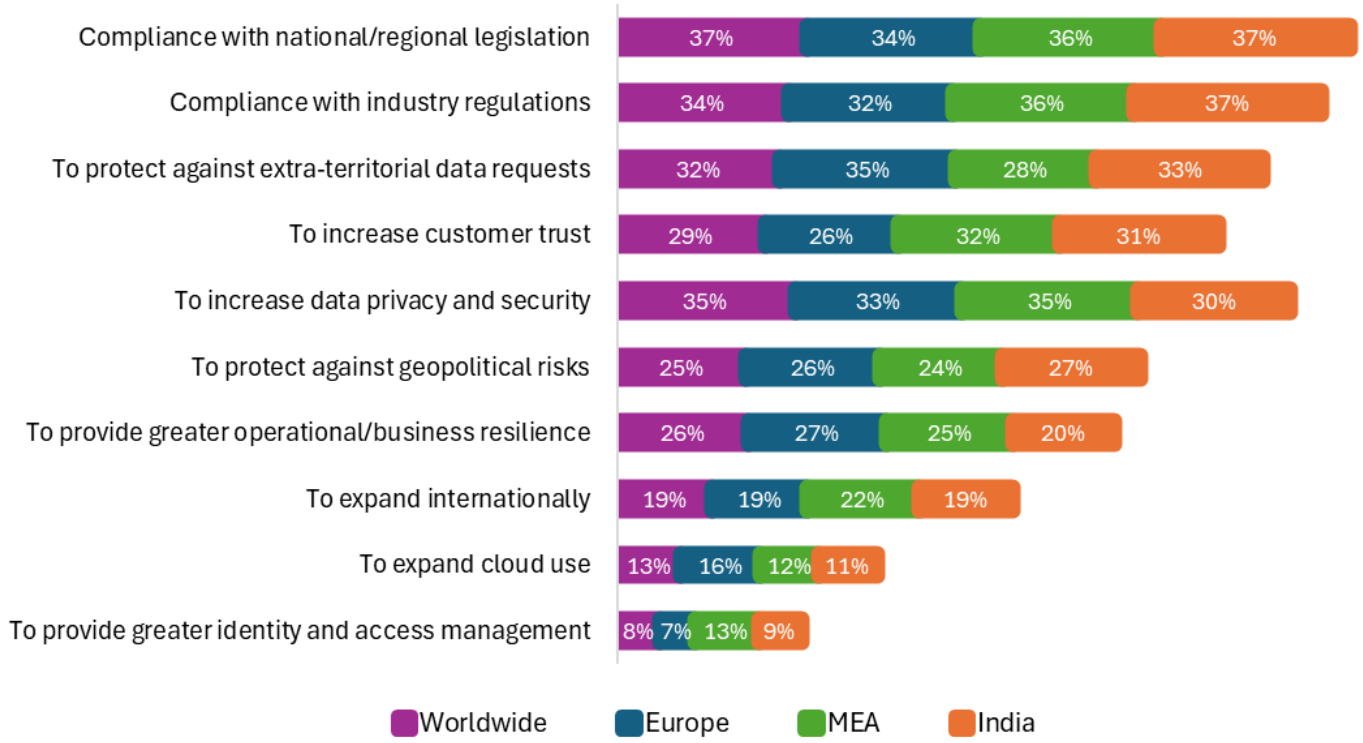
About 38% of organizations are currently using sovereign cloud solutions across MEA, while a combined 40% say they plan to use such solutions in the next 12 months or after. Their top driver is compliance, either with industry regulations or national/regional legislation. The need to increase customer trust is also seen as a key driver in the region, and this can be one of the advantages of using a sovereign cloud as it can give organizations a competitive advantage when entering new markets. Cloud sovereignty has transitioned from a strategic ambition into a series of high-impact operational deals across the region. Saudi Arabia and the United Arab Emirates, where we see sovereign cloud usage currently standing at 47% and 43%, respectively, are currently more mature, leveraging their advanced digital ecosystems to move beyond policy frameworks into the deployment of localized, mission-critical infrastructure.

India: Compliance, Guarding Against Extra-Territorial Data Requests, and Boosting Customer Trust are Key

According to IDC research, 39% in India are currently using sovereign public cloud solutions while 31% say they plan to use such solutions within 12 months. A further 13% also plan usage but not in the next 12 months. The top industry sectors that are currently using sovereign cloud in India include software and information services, followed by government, healthcare and telecoms. Figure 3 shows what's driving all organizations, and it should be noted that sovereignty is of interest to all industries, not just those that are regulated.

FIGURE 3

The Main Drivers Behind an Organization's Decision to Use Sovereign Cloud



n = 955 (Worldwide), n = 370 (Europe), n = 125 (MEA), n = 80 (India)

Source: IDC Europe's Worldwide Digital Sovereignty Survey 2025

In line with the worldwide figures, legislative and regulatory compliance are the top drivers in India. But it's also worth noting that protection against extra-territorial data requests also features in the top three, and this is followed by the need to increase customer trust as opposed to the need to increase data privacy and security which is cited as the second biggest driver globally. These are, therefore, the requirements sovereign cloud providers in India need to prioritize when addressing key market needs.

For most organizations that are currently using sovereign public cloud solutions, leveraging public cloud infrastructure from global cloud service provider that offer add-on sovereign controls for security and compliance is the preferred venue. But for most of those planning sovereign usage in the next 12 months, local cloud infrastructure and a platform delivered by global cloud service provider is the top choice. This means partnerships between global players and local providers will attract greater interest in India's sovereign cloud market.

USING A SOVEREIGN CLOUD

When to Use a Sovereign Cloud

Not all workloads need to be moved to a sovereign cloud. The data organizations should consider for migrating are primarily those that are subject to regulatory control. They should also consider using sovereign cloud for any data they classify with a high sensitivity rating. IDC has developed the following framework to help organizations implement solutions for digital sovereignty:

- **Take stock:** One of the first steps for organizations is to conduct a review of everything they will need for digital sovereignty. This will include looking at what skills will be needed for implementing, operating, and maintaining sovereignty, assessing the infrastructure and platforms that will be required to support the implementation, and reviewing cybersecurity.
- **Determine your degree of data sensitivity:** This next phase is crucial and complex, as it will require organizations to classify their data according to sensitivity ratings, 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 – of leaked or compromised, these are the data that are likely to have catastrophic consequences on a business. More than a quarter of organizations 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, organizations will need to 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 the data protection officers. This can be supported by dedicated APIs and AI.
- **Stay secure, stay sovereign:** Cybersecurity should be a shared responsibility between the organization and its sovereign services provider. In the case of sovereign cloud, it is down to the user organization to ensure 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 organizations must seek out vendors that have all the credentials and expertise needed to maintain sovereign controls for cybersecurity. Indeed, all parties and their partners should ensure that they remain sovereign today and tomorrow, which again emphasizes the need to constantly monitor the regulations and legislation that apply to an organization's industry sector and market.
- **One size does not fit all:** Sovereign solutions are not limited to one archetype. They are a range of alternatives that can typically include: public cloud with sovereign controls; logically and physically separate computing environments dedicated to a country or an industry; managed sovereign clouds where global cloud and platform

service providers partner with systems integrators or telecom service providers; solutions built, owned and operated by cloud and platform services providers headquartered in the region or country; private cloud and air-gapped offerings. These different archetypes have different costs, capabilities, levels of controls. Senior IT leaders need to constantly engage with the market and get advice to select the sovereign cloud archetypes and vendors that best fit their architectural roadmap.

Workloads to Consider for Migration

Once organizations 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.

The top three workloads that organizations globally have either already migrated or plan to migrate include data management (31%), back-up/recovery (31%), and back-end business apps (27%). There are some regional variations here. In Europe, back-up/recovery is the top workload selected by our survey respondents, while in MEA, the preference is for data management.

In India, back-up/recovery is the top answer. This highlights the significance of operational resilience as a sovereign cloud benefit and indeed the ability to continue business in the face of geopolitical threats is considered a key tenet of the overall concept of digital sovereignty.

This is followed by storage which is to be expected in markets that are only just beginning to set out on their digital sovereignty journeys as this is typically kickstarted by the enactment of local data privacy laws that require localised data storage and the extra protections that sovereignty affords. It's worth noting that both back-up/recovery and storage represent infrastructure as a service (IaaS). Again, this is to be expected during the early developmental stages of not just a sovereign cloud market but all cloud markets where organizations are still at day one of their cloud migrations which require initial investments in IaaS.

The third most likely workload for organizations in India is data management. Once users start to establish the infrastructure they need for sovereignty, the next stage of the journey, as referenced in our suggested framework above, is the need to constantly manage their data in a sovereign cloud. This then shifts the focus away from IaaS to PaaS and then on to SaaS workloads such as back-end business apps and AI/machine learning services as users begin to mature in their sovereign cloud usage.

How a Sovereign Cloud Fits into the IT Environment

When asked what percentage of their data they have classified as having high or medium sensitivity, the top answer for those in India was 21-30%. However, this is expected to

increase to 31-40% in 12 months which means organizations in the country will have more sensitive data that can be considered for migration to a sovereign cloud. And the IT venue that they are most likely to use for storing that data is a public cloud from a global provider.

However, IDC expects a slight shift here over the next 12 months as organizations will lean more toward a dedicated sovereign cloud or, in the absence of this, show a greater interest in keeping their IT on-premises.

Indeed, what may come as a surprise is that when asked how a sovereign cloud fit into their cloud strategy, the top answer for 37% of organizations globally is that they use on-premises IT and a sovereign cloud is, or will be, the *only* type of cloud we use. This is slightly higher in Europe at 38% and higher still in MEA at 41%. In India 35% also selected this response. The industry sectors in the country where this attracted the highest number of responses include retail, manufacturing as well as transportation and leisure – all sectors that can be regarded as cloud laggards that still have a lot of legacy IT infrastructure on-premises that is either too costly or complicated to migrate to cloud at present.

Most organizations 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, including in India where 54% of organizations indicated that a sovereign cloud will be part of their hybrid cloud/multicloud approach.

Budgeting for Sovereign Cloud

High cost remains one of the main challenges to be addressed when implementing digital sovereignty solutions, and all the economic uncertainties seen in recent years, especially in 2025, have clearly taken their toll on sovereign cloud budgets. 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 also the top answer selected by 35% of respondents in MEA, as well in Europe, albeit slightly higher at 39%.

In India, it is less. Here the top answer for 32% is allocating just 1-5%. Thus, despite growing demand for digital sovereignty, organizations are unwilling to pay premiums for solutions. Indeed, many are unwilling to pay anything extra with some even going so far as to agree that these should be built into all cloud platforms as a free offering. This is especially true in India when it comes to spending on solutions for operational where 16% say they expect to be free offerings built-into all cloud platforms by default.

In addition to IT budgetary constraints, organizations worldwide come up against additional costs when implementing digital sovereignty solutions. These include additional investments in specialist skills and talent, redesigning internal processes and mechanisms to ensure compliance, local infrastructure and platforms, and new tools for data governance and management.

Which Solution? One Size Does Not Fit All

Most of the major global cloud players now offer sovereign cloud solutions. These broadly fall under two categories. Firstly, there are those that we can consider as 'designed for sovereignty'. These are purpose-built for the sovereign cloud market and branded as such. The second category is 'sovereign by design'. Vendors that offer these solution types 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 that sovereign cloud is more optimally delivered via private clouds offered by partners. While sovereign partnerships are laudable, IDC's latest research shows that only 11% of organizations across the world look for sovereign cloud services delivered exclusively via private cloud.

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

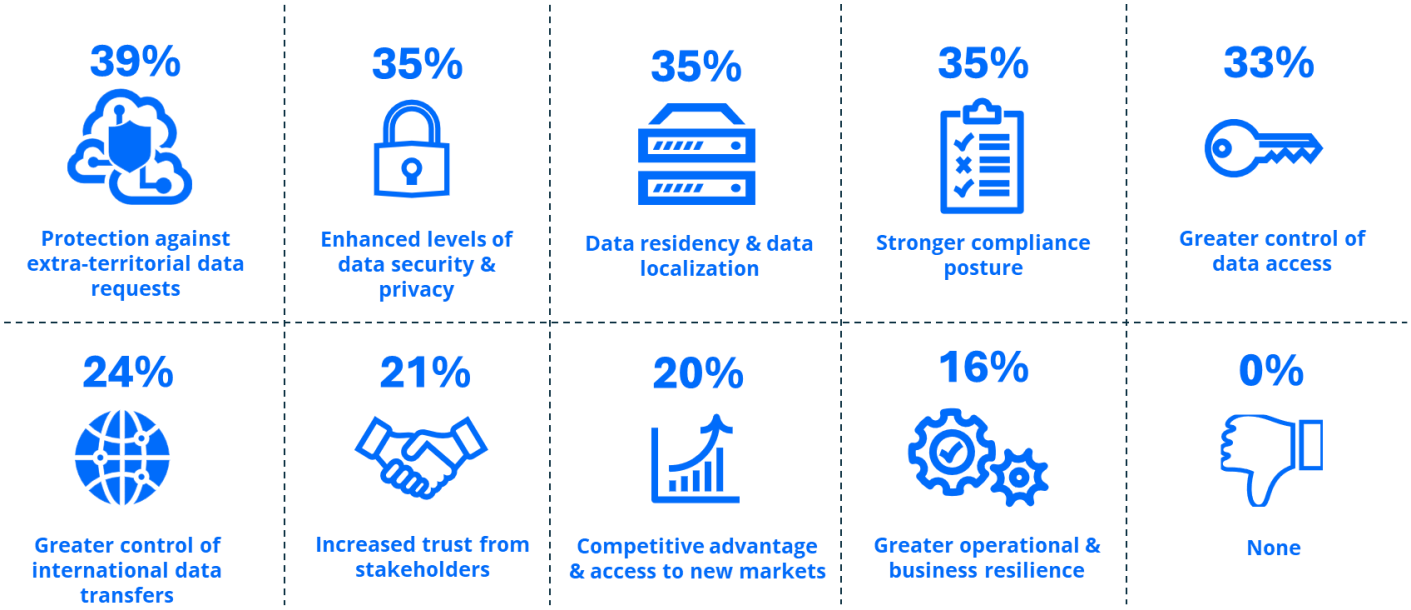
What should be clear here is that one size does not fit all industries in all markets. It is therefore crucial to work with sovereign cloud partners and providers that offer:

- Expertise and an understanding of what specific industry users need in order to develop customized 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

As with all enterprise digital initiatives, digital sovereignty solutions such as sovereign cloud should be regarded as a means to an end. Cloud is an operating model, and organizations should begin by considering the business outcomes they aim to achieve by implementing such a model. Consequently, as well as expert vendors who can help deal with their challenges, organizations should also seek sovereign cloud partners who can support them with achieving their stated business goals and perceived benefits of using sovereign cloud. Figure 5 shows the responses from those in India when asked what the main benefits that sovereign cloud has brought, or could bring, to their organization.

FIGURE 5

The Potential Benefits of Using Sovereign Cloud



n = 955 (Worldwide), n = 80 India

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

The Sought After Attributes of Sovereign Cloud Providers and Partners

As shown in Figure 5, organizations consider data residency and data localization as one of top benefits of using sovereign cloud. Consequently, the number 1 attribute they look for when selecting a sovereign cloud partner is ownership of in-country datacenters to support data localization. In India, this is the case for 59% of IDC survey respondents. Some may disagree that actual ownership is not a vital part of sovereignty, but 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 extra-territorial requests or any other unauthorized access. For those organizations who believe local data should be held on local soil by local providers, this is also likely to include ownership of the datacenters as part of achieving sovereignty.

When to Consider a Global or Local Provider

All of the above does not mean organizations only look for local players who only cover the national or regional market. Only 18% of organizations 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 local service providers, this means partnering global players to help deliver innovation and scalability. Global SaaS providers must also be able to work across the board to develop and deliver customized offerings within sovereign frameworks.

The Importance of Open Source

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 organizations 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. There is certainly a greater push for such solutions in the European Union with a growing number of alliances and initiatives to promote the use of open source to help Europe build its own homegrown IT solutions as a stronger alternative to the extra-territorial global providers. However, 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 organizations must ensure that they balance the need for sovereignty with their need for innovation.

WHAT DOES SOVEREIGN CLOUD SUCCESS LOOK LIKE?

There are several pitfalls to watch out for.

- **High complexity and high costs** consistently rank in IDC research as the two main challenges organizations face when implementing a sovereign cloud.
- **Complexity often 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. In India, 29% cited this as their main obstacle, making it the second biggest challenge compared to the global average.
- **The complexity becomes 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 26% in India.
- **Ongoing compliance monitoring across ecosystems** of sovereign solution partners and providers add to complexity, especially for multinational organizations.

- **For most organizations, specialist skills are required**, aside from overall cloud and security know-how. These include technical specialists with expertise in data management and governance and some degree of jurisprudence. The top 5 skills for organizations globally are data management and 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).

Sovereign cloud success will require working with trusted partners who can help define the strategy, secure budgets, and win corporate mindshare. Trust is a vital tenet of digital sovereignty, and it is not only applicable to the main sovereign cloud vendor but also to the 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 more than a fifth of organizations in India, for which finding trustworthy partners is their greatest hurdle.

Advice for Sovereign Cloud Users

- **Not all workloads need to be migrated to a sovereign cloud.** Organizations 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.
- **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. Organizations 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 organization's need for sovereignty and its desire to harness cloud's innovation potential.
- **Ensure security for data in transit across networks.** Some 18% of organizations 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. Organizations should therefore seek network partners that can guarantee such controls.

- **Ensure data interoperability.** Solutions that lead to vendor lock-in will restrict customers' data maneuverability. Open source solutions lend themselves well to data interoperability, portability, and transferability, which is key to sovereignty success.

MESSAGE FROM THE SPONSOR

Sovereign cloud has emerged as a strategic foundation for governments and regulated enterprises seeking to protect sensitive data, preserve national autonomy, and accelerate digital innovation with confidence.

HPE and TCS bring together complementary strengths to enable a comprehensive path to IT sovereignty. TCS SovereignSecure Cloud delivers an open, interoperable cloud stack integrated with TCS's industry solutions, E2E managed services, and built-in compliance frameworks to support PaaS, AI, GPU infra, and regulated workloads within national boundaries. HPE complements this with its trusted, sovereign-ready infrastructure through its GreenLake portfolio and Sovereign AI Solutions — designed with hardened security standards, national data residency safeguards, and resilient, AI-ready architectures

Together, TCS and HPE empower organizations to maintain operational control, ensure meet regulatory compliance requirements, and build digitally sovereign ecosystems that are resilient, scalable, and innovation-led.

Explore how HPE and TCS can help accelerate your sovereign cloud journey with confidence. Read about TCS SovereignSecure Cloud, HPE AI Factory Sovereign, and HPE GreenLake.

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.).

Global headquarters

One Beacon Street
Suite 33100
Boston, MA 02108
USA
508.872.8200
X: @IDC
blogs.idc.com
www.idc.com