THE JOURNEY TO

CLOUD SOVEREIGNTY

ASSESSING CLOUD POTENTIAL TO DRIVE TRANSFORMATION AND BUILD TRUST

#GetTheFutureYouWant

Capgemini RESEARCH INSTITUTE

Introduction

The COVID-19 pandemic has turbo-charged cloud adoption. In an unprecedented business environment, cloud services have proven crucial to remote-workforce collaboration and productivity, disaster recovery, cost control, agility, resilience, and business continuity. However, as cloud adoption has accelerated, we have also seen a shift in attitudes toward cloud, notably regarding its impact on "sovereignty" issues such as the need for data to be subject to the laws of the country/regions in which it is collected or in which it is processed.

Sovereignty has gained a new prominence as a result of the pandemic, which has revealed significant vulnerabilities in complex international supply chains and has emphasized the role of critical data such as health. National governments and businesses have not only questioned the security of physical supply chains, but also where exactly their data is stored in the cloud, and what control they have over service capacity and availability in the event of a burst of demand, or in events of security incidents. Concerns around cloud sovereignty – including data, operational, and technical issues – are not new and have been gaining impetus over the past few years. However, it is a subject that is now under increasing scrutiny because of rising geopolitical tensions; changing data and privacy laws in different countries; the dominant role of cloud players concentrated in a few regions; and the lessons learned through the pandemic. As a result, governments and organizations are re-evaluating their external exposure and looking for ways to maintain physical and digital control over strategic assets, including data, algorithms, and critical software.

We wanted to look deeper into organizational awareness and key priorities when it comes to cloud sovereignty, and the role it plays in overall cloud strategy. We also wanted to provide pragmatic recommendations for operating successfully in this evolving landscape. We surveyed executives from 1,000 organizations, and also analyzed more than 50 cloud sovereignty use cases, assessing their growth potential, complexity, and the benefits they offer.

Introduction

This report focuses on four key areas:

01

Examining how demand for data and cloud sovereignty is gaining impetus on two fronts: from the regulatory side and from organizations' pivoting to cloud strategies.

02

Assessing what organizations today consider a "sovereign cloud" and which elements of sovereignty they are prioritizing.

03

Profiling the use cases that offer the maximum potential and where organizations are focusing their efforts.

04

Finally, drawing on best practices in this emerging environment, outlining key recommendations for organizations wishing to formulate their "move-to-sovereign" strategy.

Elements of Cloud Sovereignty

Cloud sovereignty focuses on a cloud-computing environment that is owned, deployed, governed, and managed locally or regionally within a single nation or jurisdiction. The key idea behind sovereignty is to respond to each organization's desire for control, choice, and autonomy over their data, systems, and applications.

These requirements vary; for most, cloud and/or the party controlling the cloud, should be located within the jurisdiction and the data should not be accessible under foreign laws or from any outside geography. However, in some very stringent cases, it is obligatory for the cloud provider also to be of local origin.

There are three key areas within cloud sovereignty:

01

Data sovereignty: Allows organizations to keep control of their data in the cloud, prevent unsolicited third-party access, and maintain regulatory rules for stored data.

02

Operational sovereignty: Allows organizations to have visibility and control of their operations while maintaining continuity of operations and regulatory compliance.

03

Technical sovereignty: Allows organizations to run workloads without continuous dependence on a provider's cloud.

Elements of Cloud Sovereignty

Cloud Sovereignty

Data Sovereignty	Operational Sovereignty	Technical Sovereignty
• Data Localization: Hosting, using, storing or processing of cloud data in preferred location or jurisdiction (usually home country/region/ territory) • Data Ownership: Data is at all times under the control and ownership of its originator/ producer • Data Traceability: Focus on management and transparency of data across the lifecycle • Data Access Controls: It is about who can access the data, from where and for what purpose	• Operational Resilience: Ensuring continuity of cloud service in case of unplanned disruptions • Regulatory Compliance: Focus on alignment with region/ sector-specific regulations and laws • Sovereignty of ecosystem of partners including telcos/ network provider or API calls • Following the security objectives, controls, governance management; detection of and reaction to cyber attacks	• Portability and Reversibility: Ability to move applications and data from one cloud-computing environment to another with minimal disruption • Interoperability: Solution follows integration standards and can be easily connected to existing and/or future solutions from other providers

Note: There is no single definition of cloud sovereignty; the report outlines key elements in Capgemini's views along with the priorities highlighted by organizations.

Source: Capgemini Research Institute Analysis.

Executive summary – key takeaways

Cloud sovereignty is gaining significance among both organizations and governments

- As cloud proliferation continues, the topic of "sovereignty" is gaining importance, both from the regulatory side and among organizations themselves.
- **Sixty-nine percent** of organizations cite "potential exposure to extra-territorial laws" as a key concern in the current cloud environment. In parallel, sovereignty-related factors such as availability of local/regional data-storage centers increase in significance when organizations select a public cloud platform provider. As a result, more than 80% of organizations see cloud sovereignty continuing to gain prominence.
- Further, governments around the world are focusing on bringing in cloud sovereignty-related initiatives in their countries. For instance, European Commission (EC) has been at the forefront of rolling out initiatives that allow the region, organizations, and individuals more control, choice, and autonomy over their data, systems, and applications in the cloud.

Organizations are developing cloud sovereignty strategies with a strong focus on data localization

- Today, cloud sovereignty is driven externally, by regulation, and internally, by organizations' need to control their data. A large majority of organizations believe that they will adopt cloud sovereignty to ensure compliance with regulations (71%) or to bring in controls and transparency over their data (67%).
- Moreover, more than half (52%) of organizations are planning on including sovereignty in their overall cloud strategy in the next 12 months.
- However, currently, organizations are limiting cloud sovereignty to data localization – with 43% of organizations focusing on keeping their data within their preferred jurisdiction (usually national/regional borders), irrespective of whether the cloud provider is of local origin. Only 14% define cloud sovereignty as the exclusive use of cloud providers based in the same legal jurisdiction and storing data within the borders of a country or region.

Executive summary – key takeaways

- This shows that, despite organizational concerns around potential exposure to extra-territorial laws, only a few organizations are expecting to decouple from their current cloud providers. Rather, they are focusing on the possibilities for innovation and scale provided by hyperscalers, and are looking to their service providers to afford options for managing their sovereignty issues.
- On the supply front, cloud solutions with sovereignty-related factors are currently evolving, with developments ranging from disconnected versions to partnerships with autonomous legal entities.

Beyond data localization, organizations also expect cloud sovereignty to build trust, foster collaboration, and accelerate the move to a data-sharing ecosystem

- 60% of organizations believe that cloud sovereignty will facilitate sharing data with trusted ecosystem partners and 55% of organizations believe it offers more collaboration opportunities; 63% of organizations believe that cloud sovereignty will provide them with a secure, trustworthy environment for data storage.
- Organizations also indicate viable use cases such as collaboration-led data platforms, data exchange, and collaborative real-time monitoring to start their cloud sovereignty journey.

With the cloud sovereignty space fast emerging, organizations need to stay ahead of the curve – from understanding the emerging trends, to factoring elements of sovereignty into the overall cloud strategy, as well as ensuring technical flexibility in their cloud architecture.

Executive summary – key takeaways

We highlight four key recommendations for organizations:

Define sovereignty objectives: Identify your sovereignty objectives based on the three elements of cloud sovereignty; understand the laws of the land for digital sovereignty; track key developments in the cloud and data-sovereignty space; continuously assess risk exposure; and set up a compliance organization.

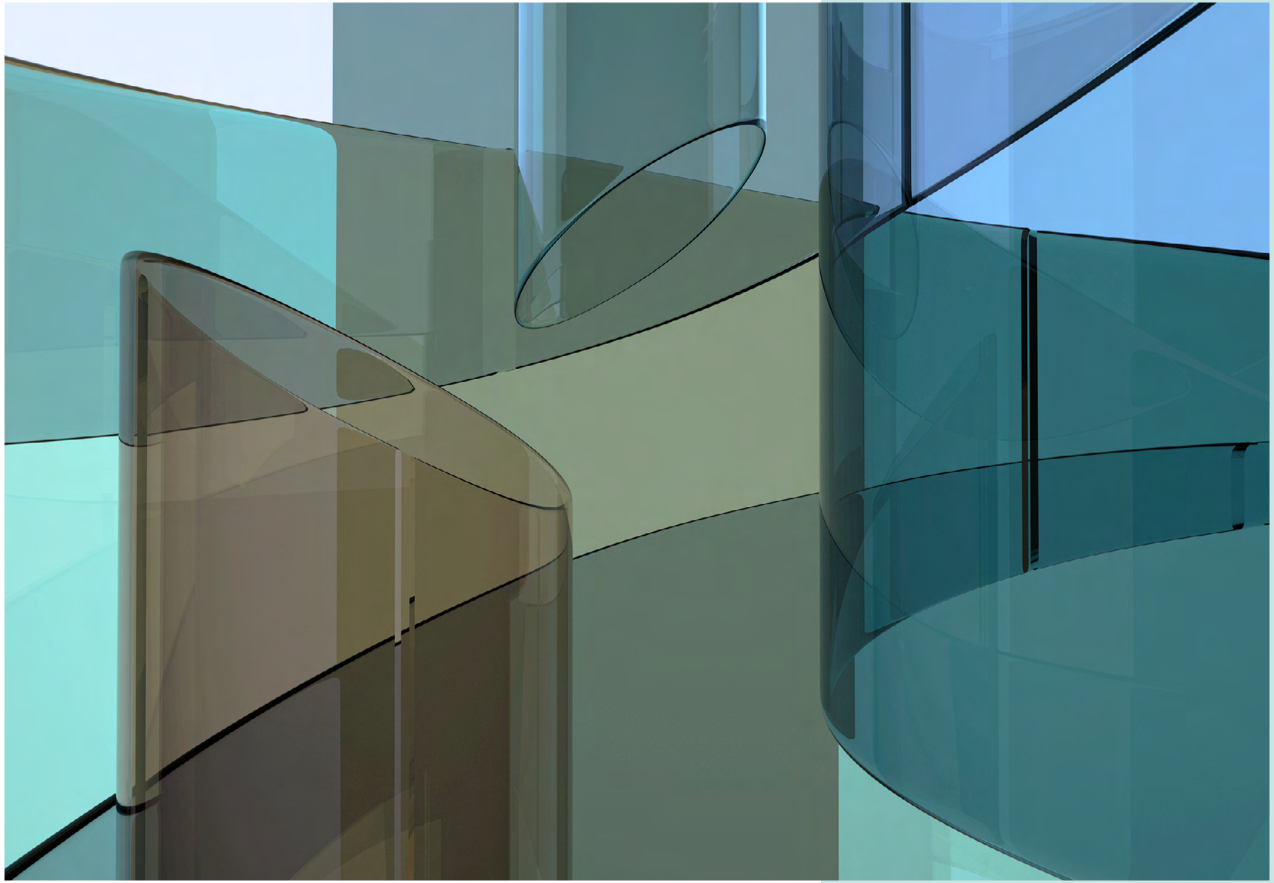
Assess cloud providers through a sovereignty lens – including data sovereignty (for data residency, controls, transparency, storage, back-ups, etc.); operational sovereignty (for security, compliance, and operational resilience); as well as technical sovereignty (to assess interoperability, migration features, and clear exit policy/ process).

Align for a flexible cloud architecture: Identify your sensitive workloads and most viable use cases; consider end-to-end encryption, as well as key management solutions. At the same time, evaluate hybrid options, and prepare for a multi-cloud architecture by understanding the potential as well as the challenges it brings.

Develop the potential of sovereign cloud by exploring its value proposition in terms of trust, security, and collaboration through ecosystem participation.

69%

of organizations cite “potential exposure to extra-territorial laws” as a key concern in the current cloud environment.



01

Cloud sovereignty is gaining prominence

Demand for cloud services in organizations is shifting in line with new expectations around sovereignty

Worldwide spending on cloud services is expected to reach $1.3 trillion by 2025 – reflecting an annual growth rate of about 16.9%.[1] For instance, US-based financial services firm, Capital One Financial, recently moved all of its data to the public cloud. Chris Nims, SVP of technology at Capital One, comments,*"We declared the cloud as our destination, which began with the declaration that anything new could only be built in the cloud. We didn't just do it in pockets … we made the declaration that we go all in."*[2]

The cloud's proliferation has brought the topic of sovereignty to the fore, from the regulatory side as well as from organizations themselves. Although organizational definitions and levels of understanding of cloud sovereignty vary widely, our research reveals that factors and concerns that are closely linked to sovereignty are gaining importance when organizations formulate their cloud strategies.

For instance, the importance of security, transparency, openness, and interoperability is reflected in the concerns that organizations have in the current cloud environment. A CEO of an Australia-based private healthcare organization, comments, *"In hospitals, your storage is enormous: you have confidential patient records and hospital information systems such as PACS (the Picture Archiving and Communication System), with all the medical details on patients. Here, cloud has a lot of benefits, as it gives doctors and nurses easy access to prescribe or check on their patient from their home or anywhere. However, it is a threat if this data gets into the hands of a non-authorized entities, which can be a possibility if it is a non-sovereign cloud environment. This is a big concern among many healthcare CEOs today."*

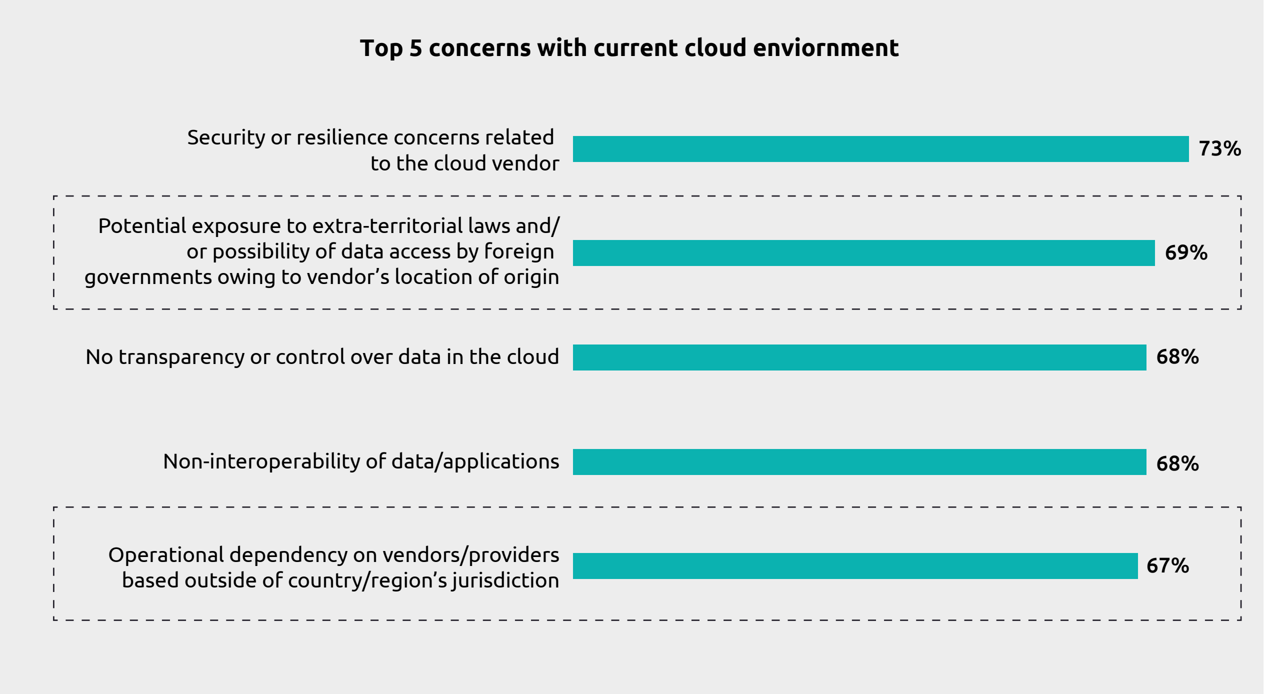
As Figure 1 shows:

- 69% of organizations are concerned about potential exposure to extra-territorial laws in a cloud environment. This is even more pronounced in sectors such as industrial manufacturing (75%) and life sciences (74%), and specifically in European countries such as Italy (75%), Sweden (72%), and Spain (71%).
- 73% of organizations across sectors – 79% in industrial manufacturing and 74% in the public sector – have security or resilience-related concerns with public cloud vendors. The security concerns can be attributed to increased dependency of organizations on cloud vendors. Our research shows that 67% of organizations are concerned about operational dependency on vendors/providers based outside the country's jurisdiction.

In parallel, organizations are becoming cautious about how to control the flow of data across boundaries and how to contain data in certain regions within the cloud environment. Our research shows that factors related to sovereignty are gaining influence when organizations are selecting a public cloud platform provider. As the director from a leading industrial automation firm states,

Fig.1

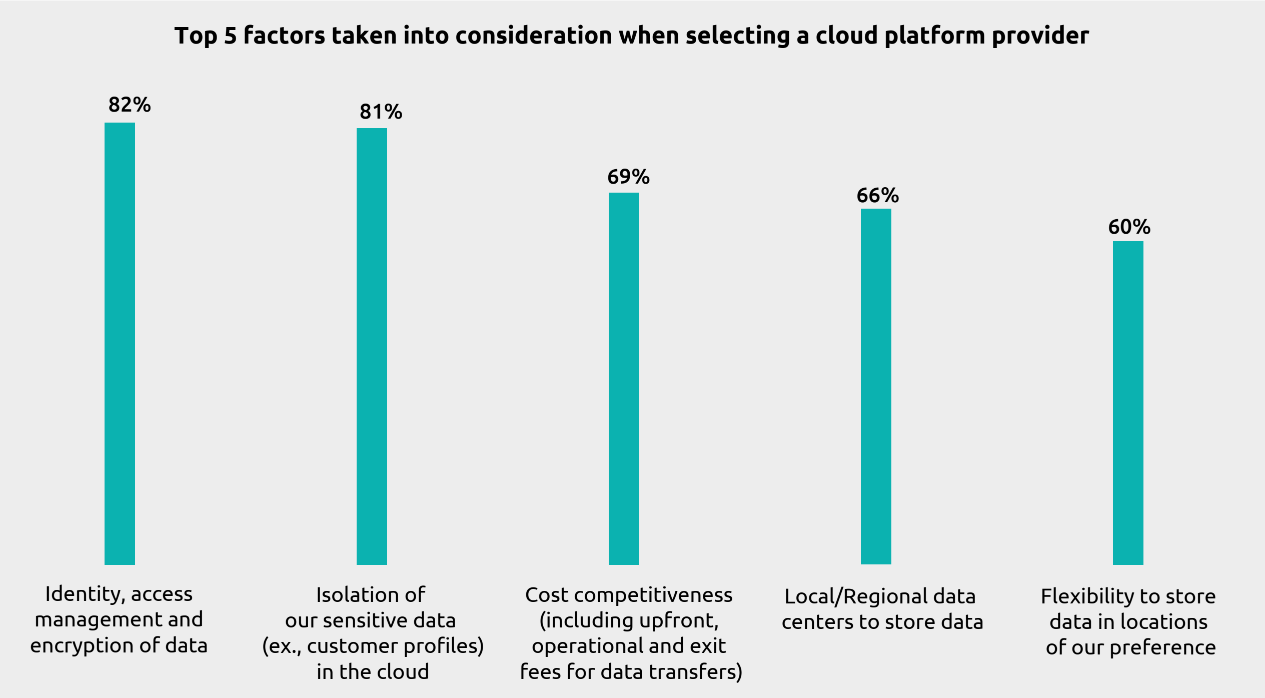
Organizations cite sovereignty-related concerns in the current cloud environment



Source: Capgemini Research Institute, Cloud Sovereignty Survey, May–June 2021, N = 1,000 organizations.

Fig.2

Organizations are giving importance to sovereignty related factors when selecting cloud platform providers.



Source: Capgemini Research Institute, Cloud Sovereignty Survey, May–June 2021, N = 1,000 organizations.

"When selecting a cloud provider, the key factors to consider include: Where is the data stored? Is the data safe and secure? Is it encrypted at rest and when in transit? And the longevity of the data and also audit: Is that company getting audited? Is there a third-party auditor that audits the safety and security of the data and, most of all, is there vendor transparency? Transparency is very important because, if the data gets subpoenaed by an agency or federal government, it is necessary to be informed that the government agency is asking for data about the company."

As Figure 2 shows, when selecting cloud service providers:

- 82% of organizations consider factors related to identity, access management, and encryption. This increases to 88% for insurance and 87% for industrial manufacturing.
- 81% consider isolation of their sensitive data in the cloud. In the life sciences sector, 84% of organizations consider this to be a key factor.
- 66% of organizations globally and in the public sector consider local/regional data-center offerings of cloud vendors to be a key selection criterion.

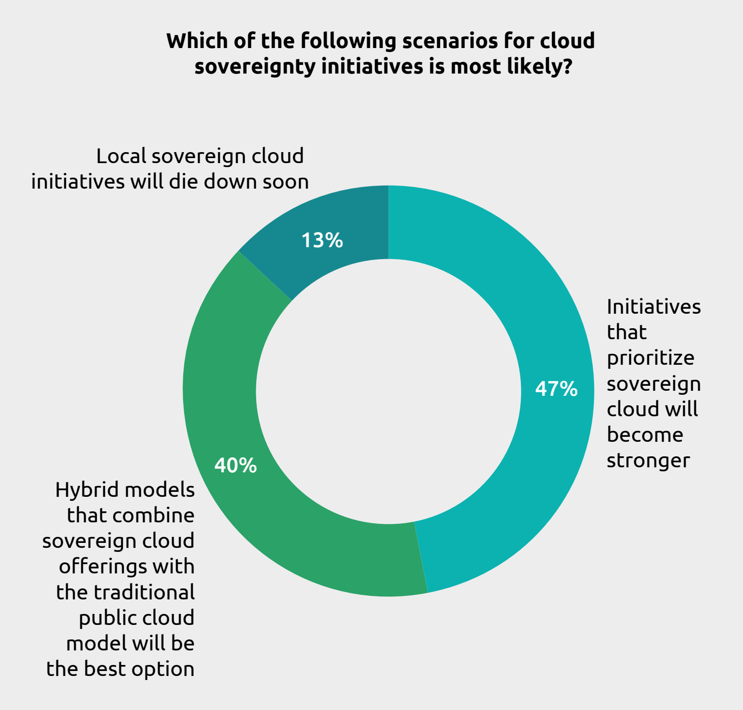
Organizations anticipate intensifying demand for cloud sovereignty

The majority of organizations in our research say that cloud sovereignty is not a passing trend: only 13% of organizations predict that interest in cloud sovereignty will fade in the short term (see Figure 3). It is interesting that 40% of organizations also foresee the emergence of hybrid models that combine a sovereign offering with the traditional public cloud offering.

The director of a leading industrial automation firm shares this sentiment, *"With new regulations and legislation emerging, I believe that the global sovereignty landscape will become stronger, but I don't think it can be 'too' stringent. I believe hybrid models, multi-cloud environments, and the move into the edge environment will be the key characteristics of cloud sovereignty."*

Fig.3

A majority of organizations see cloud sovereignty gaining importance in the future, either as standalone solutions, or through hybrid models



Which of the following scenarios for cloud sovereignty initiatives is most likely?

Source: Capgemini Research Institute, Cloud Sovereignty Survey, May–June 2021, N = 1,000 organizations.

Certain countries clearly expect sovereign initiatives to become stronger: 65% of organizations in the UK; 61% in Italy; 51% in France, Germany, and Spain; and 49% in Australia expect sovereign initiatives to dominate; whereas 70% in the US and 66% in India expect hybrid models to emerge.

87%

of organizations see cloud sovereignty continuing to gain prominence.

Governments and regulatory bodies across the world are focused on cloud sovereignty issues

With the exponential growth of data crossing borders, many geographies and governments wish to have more control, transparency, choice, and flexibility over how their data and applications are handled in the cloud. This, in turn, is creating tensions between different countries' needs and wants:

- The US introduced the Clarifying Lawful Overseas Use of Data (CLOUD) Act in March 2018. It gives US law-enforcement authorities access to data belonging to US-based cloud service providers, regardless of where it is stored.[3] Non-US firms are also subject to the CLOUD Act if they are a subsidiary of a US cloud or IT service provider, even if headquartered outside of the US. This has been a key concern for non-US geographies and governments, specifically Europe.
- In July 2020, under the Schrems II ruling, the European Court of Justice (ECJ) struck down the "privacy shield" – an agreement that provided a legal basis for transfers of personal data between the EU and the US. The EU ruled that the privacy shield did not provide adequate protection to EU citizens. As an aftermath of the Schrems II ruling, the European Commission adopted new sets of Standard Contractual Clauses (SCC) in the GDPR in 2021 to ensure appropriate data protection safeguards for international data transfers and address controller-processor obligations.[4]

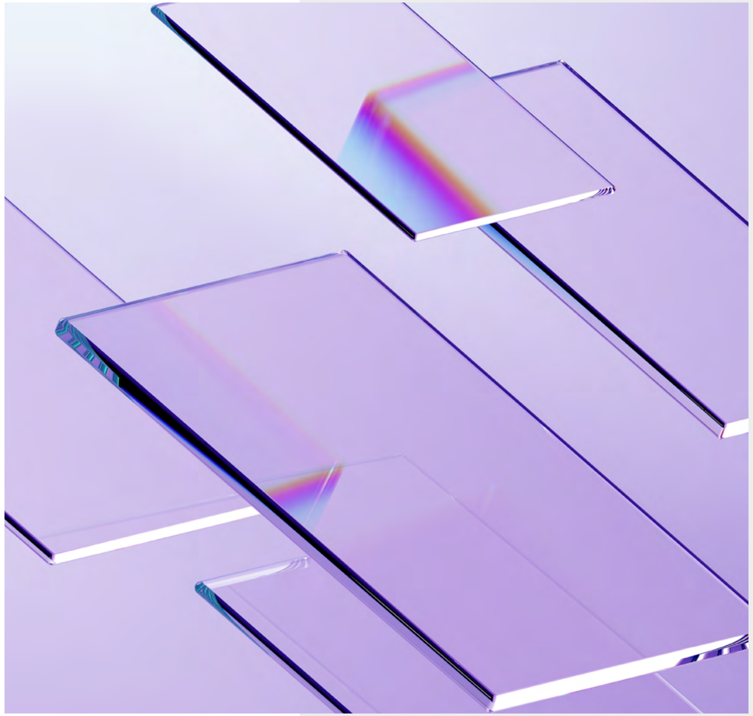
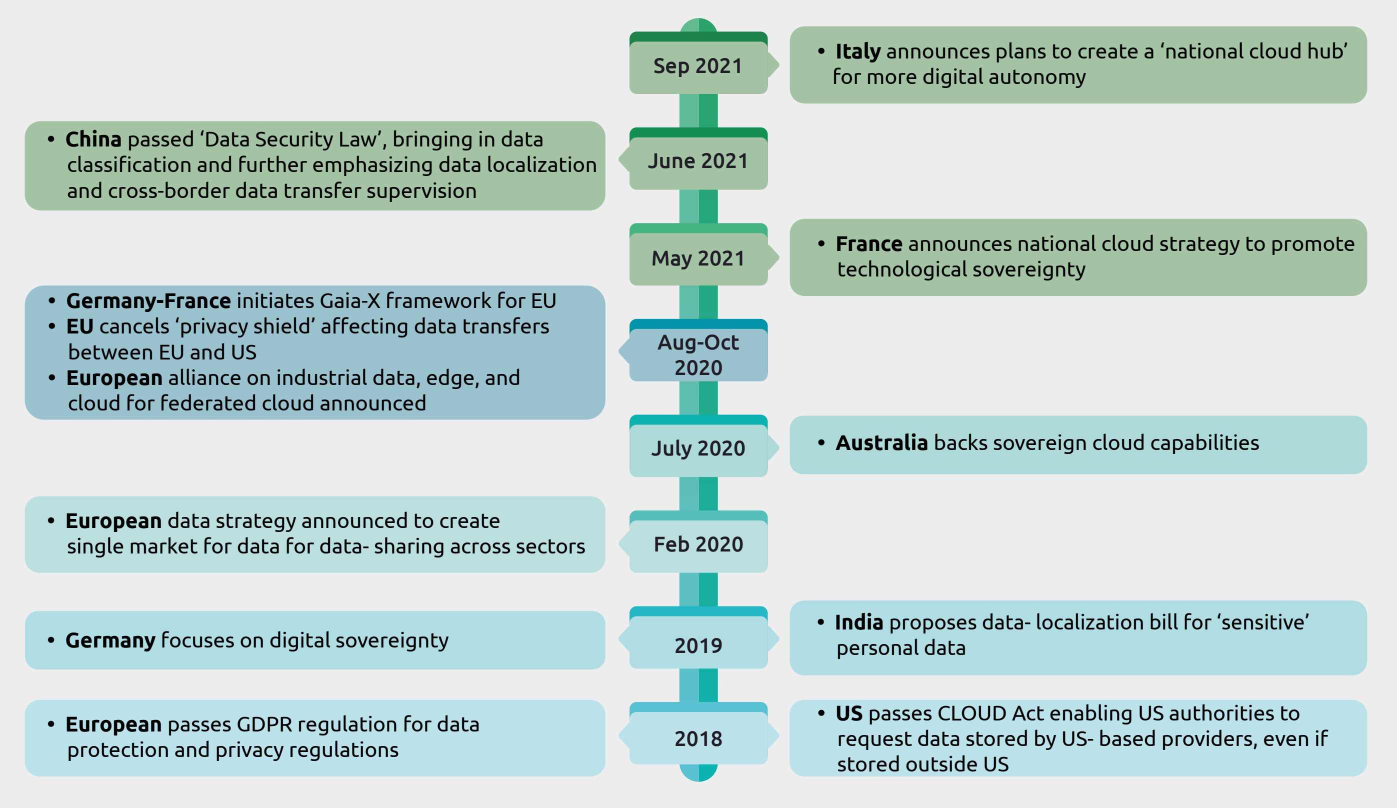


Fig.4

A timeline of key developments across different countries



Sep 2021
- **Italy** announces plans to create a 'national cloud hub' for more digital autonomy

June 2021
- **China** passed 'Data Security Law', bringing in data classification and further emphasizing data localization and cross-border data transfer supervision

May 2021
- **France** announces national cloud strategy to promote technological sovereignty

Aug-Oct 2020
- **Germany-France** initiates Gaia-X framework for EU
- **EU** cancels 'privacy shield' affecting data transfers between EU and US
- **European** alliance on industrial data, edge, and cloud for federated cloud announced

July 2020
- **Australia** backs sovereign cloud capabilities

Feb 2020
- **European** data strategy announced to create single market for data for data- sharing across sectors

2019
- **Germany** focuses on digital sovereignty
- **India** proposes data- localization bill for 'sensitive' personal data

2018
- **European** passes GDPR regulation for data protection and privacy regulations
- **US** passes CLOUD Act enabling US authorities to request data stored by US- based providers, even if stored outside US

Note: The timeline is an indicative list of sovereignty-related initiatives from different countries and is not an exhaustive representation.

Source: Capgemini Research Institute Analysis.

Below, we look at key developments across a number of blocs and countries:

European Commission

In 2018, Europe passed the General Data Protection Regulation (GDPR) to bring in high levels of data protection and privacy regulation and to give individuals more control over their data. Since then, the European Commission (EC) has been at the forefront of initiatives to allow the region, organizations, and individuals more control, choice, and autonomy over their data, systems, and applications in the cloud. For instance, EC and German Presidency of the Council of the European Union announced their initiative to build their "next-generation cloud" for Europe to build trustworthy data infrastructures for public services, businesses, and citizens in Europe.[5]

Key developments include:

- **European data strategy:** In early 2020, the European data strategy was introduced to create a single European data space for data exchange and sharing within the EU and across key sectors affording data

owners increased control of their data while being subject to EU rules related to data privacy and protection.[6]
The EU data strategy also includes investing close to €2bn in "European high-impact projects" to develop data-processing and data-sharing infrastructure projects ultimately leading to trustworthy cloud environments.[7]

- **EU Cloud federation to enhance spending:** Towards late 2020, the EU announced spending of up to €10bn between 2021 and 2027 to build a European alliance on industrial data, edge, and cloud. The purpose of the alliance is to create a federated European cloud with joint investments in cloud infrastructure and services. It also aims to create a European marketplace for cloud services that will act as a single repository for all cloud services. The idea is also to build an EU cloud rulebook for cloud services to provide a single framework on best practices for cloud use.[8,9]

A recent communication from the EC states, *"Today, data produced in Europe is generally stored and processed outside Europe, and its value is also extracted outside Europe. While businesses generating and exploiting data should retain free choice in this regard, this can bring risks in terms of cybersecurity, supply vulnerabilities, switching possibilities, as well as unlawful access to data by third countries."*[10] It also refers to doubling the percentage (from 21% currently) of organizations using advanced cloud services by 2025.

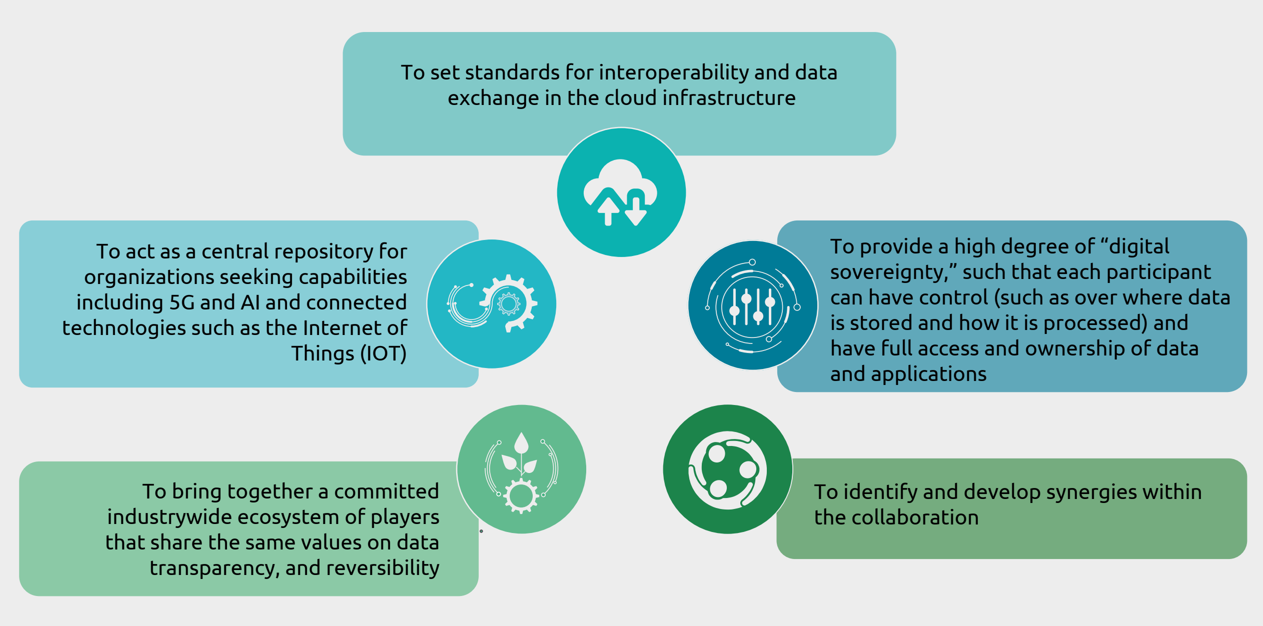
In February 2022, EC also published its proposal for the "EU Data Act" – a regulation which aims to provide a harmonized framework for data sharing, cloud switching, and international transfers of non-personal data.[11]

GAIA-X for industry-wide commitment, initiated in the EU:

In September 2020, GAIA-X, a public/private consortium initiative comprising cloud suppliers, businesses, and the public sector, was established to create a unified ecosystem of cloud and data infrastructure and services for the EU, based upon open source and open standards for EU. Figure 5 highlights some of the key features of the GAIA-X framework.

Fig.5

GAIA-X aims to set standards, enhance collaboration, and provide digital sovereignty to organizations in the EU



To set standards for interoperability and data exchange in the cloud infrastructure

To act as a central repository for organizations seeking capabilities including 5G and AI and connected technologies such as the Internet of Things (IOT)

To provide a high degree of "digital sovereignty," such that each participant can have control (such as over where data is stored and how it is processed) and have full access and ownership of data and applications

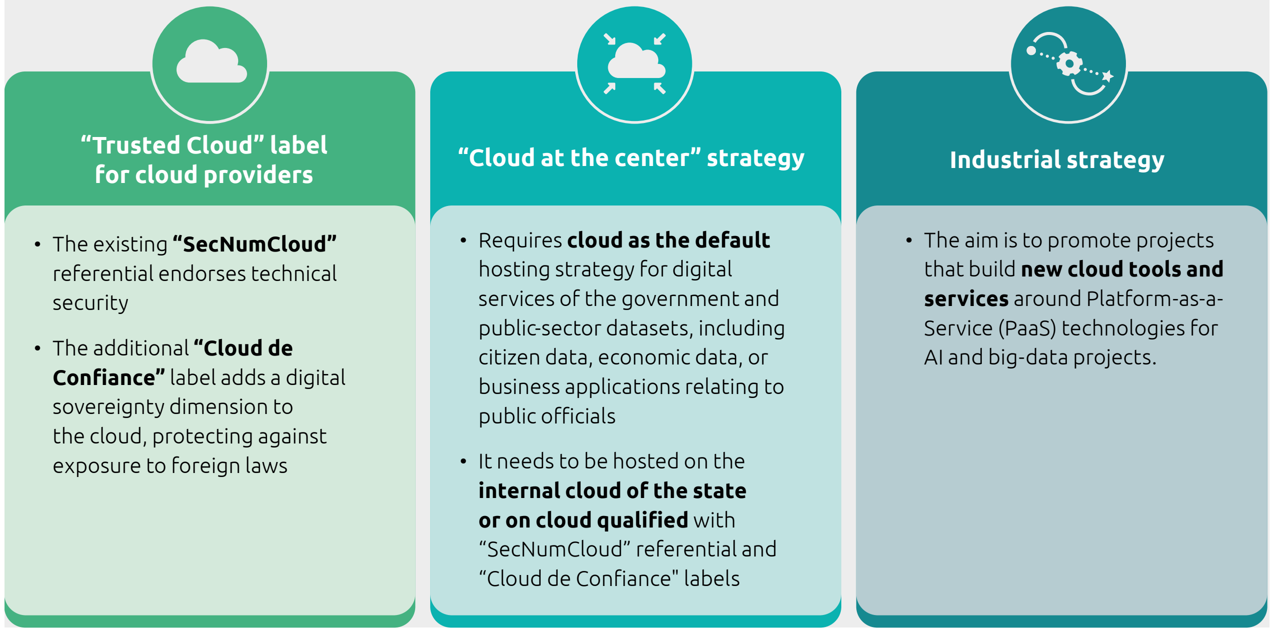
To bring together a committed industrywide ecosystem of players that share the same values on data transparency, and reversibility

To identify and develop synergies within the collaboration

Source: GAIA-X.

Fig.6

France's national cloud strategy is focused on three pillars:[12,13]



"Trusted Cloud" label for cloud providers

- The existing **"SecNumCloud"** referential endorses technical security
- The additional **"Cloud de Confiance"** label adds a digital sovereignty dimension to the cloud, protecting against exposure to foreign laws

"Cloud at the center" strategy

- Requires **cloud as the default** hosting strategy for digital services of the government and public-sector datasets, including citizen data, economic data, or business applications relating to public officials
- It needs to be hosted on the **internal cloud of the state or on cloud qualified** with "SecNumCloud" referential and "Cloud de Confiance" labels

Industrial strategy

- The aim is to promote projects that build **new cloud tools and services** around Platform-as-a-Service (PaaS) technologies for AI and big-data projects.

Source: Numerique.gouv.fr, Cloud au centre.

France announces national cloud strategy to promote technological sovereignty:

In May 2021, France announced its national cloud strategy (see Figure 6).

Germany strengthens the digital sovereignty of public administration

In Germany, federal, state, and local governments have set themselves the goal of maintaining and continuously strengthening the digital sovereignty of public administration. With the establishment of the Cloud Computing and Digital Sovereignty working group by the IT Planning Council in 2019, a fundamental framework was created for coordinating the project to strengthen the digital sovereignty of public administration in Germany.[14] Parallelly, German Federal Ministry for Economic Affairs and Energy (BMWi) also initiated "trusted cloud label" for cloud services to create transparency and build trust in cloud technologies.[15]

Also, the implementation of private cloud infrastructures and open-source solutions is a key focus area in German public administrations. For the reasons of digital sovereignty, the use of public cloud infrastructures is only possible to a limited extent. The development of two sovereign clouds for the German administration is under discussion:

- A German administrative cloud primarily based on open-source solutions is planned. In addition, public sector organizations are also planning to increase exchange of IT solutions on standardized cloud stacks through private clouds.[16]
- A sovereign cloud based on hyperscalers like Microsoft Azure with services for communication, collaboration and office functionality built on national and European requirements for information security and data protection is an additional option.[17]

On that note, Harald Joos, CIO of the Ministry of Finance, one of the driving forces behind their multi-cloud strategy, says, *"We need both – 'open source software' as well as solutions from hyperscalers. On one hand, the German public sector wants to participate in innovation and, on the other, we also have to maintain control over operations and data in order to fulfill all legal and compliance aspects. By building a German administrative cloud, we plan to strengthen the digital competence and sovereignty of the German administration. With the additional establishment of a 'Microsoft Sovereign Cloud' we are also gaining a little more sovereignty as well. With several powerful cloud operating platforms, we can also achieve our goal of climate-neutral IT production more quickly."*

In Aug 2021, T-Systems and Google Cloud partnered to build and deliver sovereign cloud services in Germany especially for the public and healthcare sector.[18]

Australian government emphasizes end-to-end sovereignty for certain datasets

The Australian government, with its "whole-of-government" hosting strategy, has published a certification framework for hosting services. The aim is to address data-sovereignty risks such as ownership, access, and control. The hosting strategy also includes creating a secure hosting ecosystem with certified data centers and network infrastructure.[19] For instance, the Canberra government has certified three local data-center providers – Australian Data Centres (ADC), Canberra Data Centres (CDC), and Macquarie Telecom – to store sensitive government data.

In addition, the government plans to consider end-to-end sovereignty for "certain datasets" that contain sensitive information relating to the Australian public. The idea is to:

- Classify them as sovereign datasets
- Host them only in Australia, using accredited local data centers and local networks, with rights of access only for the Australian government and Australian service providers
- Australian government services minister, Stuart Robert, said, *"We think there is a case, and we're exploring this now, for Australian datasets to be in Australian data centers, run by Australians with Australian providers, and securely housed and routed within Australia, to give maximum assurance to Australians that their data's safe."*[20] The New South Wales government has signed an agreement with local provider, Vault Cloud, for cloud services.[21]

Several other countries are also proposing data-localization measures:

- **Italy also plans to create a "national cloud hub"** to promote digital autonomy, which includes bringing in cloud services managed and controlled by providers from inside the EU and security certification requirements including national security for public cloud services.[22]
- **China has introduced a Data Security Law for data classification that further emphasizes data localization:** In June 2021, China introduced its Data Security Law, which requires organizations to classify their data according to importance to the national economy and public interest, such as "national core data," "important data," etc. The Data Security Law, along with the Cybersecurity Law of 2017, further emphasizes supervision of data-localization and cross-border data transfers.[23] In November 2021, "Personal Information Protection Law" went into effect in China which has implications on cross-border transfer of data.[24]
- **India has proposed data localization for sensitive data:** In 2019 India proposed a bill to initiate a data-localization framework. Sector-specific data-localization measures are already emerging in various sectors. In the telecommunications sector, organizations are required to store and process their subscriber information only within the country's borders. In financial services, the Reserve Bank of India (RBI, India's central bank) has mandated that payments data should be stored only within the country.[25]

"We need both - 'open source software' as well as solutions from hyperscalers. On one hand, the German public sector wants to participate in innovation and, on the other, we also have to maintain control over operations and data in order to fulfill all legal and compliance aspects. By building a German administrative cloud, we plan to strengthen the digital competence and sovereignty of the German administration. With the additional establishment of a 'Microsoft Sovereign Cloud', we are also gaining a little more sovereignty as well. With several powerful cloud operating platforms, we can also achieve our goal of climate-neutral IT production more quickly."

Harald Joos

CIO of the Ministry of Finance, Germany

67%

of organizations believe cloud sovereignty will be adopted to bring in more control over and transparency of their data.

02

Organizations are progressing on cloud sovereignty with a focus on data localization

Cloud sovereignty is driven by regulations and the need for control

Christophe Dufour, chief digital officer at AstraZeneca France, comments, *"Today's main challenge is around handling medical data in the cloud. In France, I would say we have strong pressure coming from both the public and authorities to protect patient data. And, today, it is a must have to use solutions that prove the data is not used without permission, and especially not outside the European territory. So, I would say that the main driver today to move to cloud sovereignty – in medical studies, in real-world data analysis – is because of the regulations such as the CLOUD Act, which does not protect national citizens from having data accessed by foreign authorities."*

In our survey, 71% of organizations believe that cloud sovereignty will be adopted to ensure compliance with regulations and standards of the nation/state/local government. For instance, in Sweden, a government digitalization organization, eSam, has ruled that outsourcing public-sector data to US cloud service providers subject to the CLOUD Act would violate the country's law on public access to information and secrecy.[26] More than half (52%) of organizations say that their decisions in relation to cloud sovereignty will also depend on their level of trust in the local government.

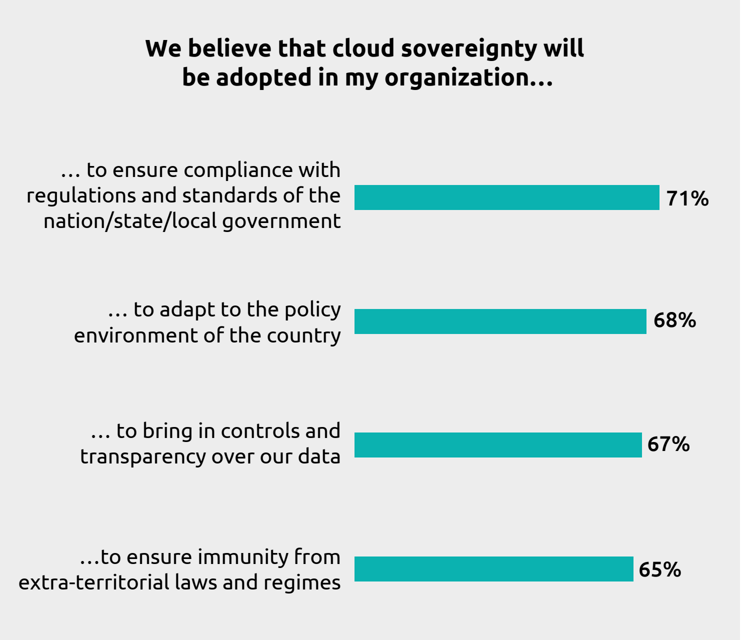
Moreover, 65% of organizations say immunity from extra-territorial data access is a key driver (see Figure 7). This shows that organizations are keen to have greater control over their data when hosted in the cloud. Our research shows that 67% of organizations believe cloud sovereignty will be adopted to bring in more control over and transparency of their data.

71%

of organizations believe that cloud sovereignty will be adopted to ensure compliance with regulations and standards of the nation/state/local government.

Fig.7

Compliance and control needs are the key drivers for organizations to look at cloud sovereignty



Note: Top four represented.
Source: Capgemini Research Institute, Cloud Sovereignty Survey, May–June 2021, N = 1,000 organizations.

"Today's main challenge is around handling medical data in the cloud. In France, I would say we have strong pressure coming from both the public and authorities to protect patient data. And, today, it is a must have to use solutions that prove the data is not used without permission, and especially not outside the European territory. So, I would say that the main driver today to move to cloud sovereignty – in medical studies, in real-world data analysis – is because of the regulations such as the CLOUD Act, which does not protect national citizens from having data accessed by foreign authorities."

Christophe Dufour

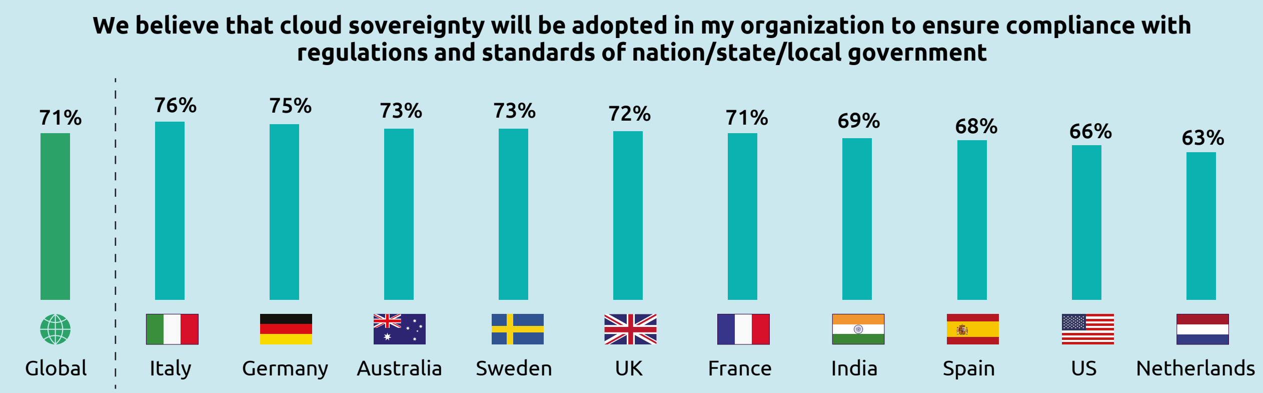
Chief digital officer at AstraZeneca France

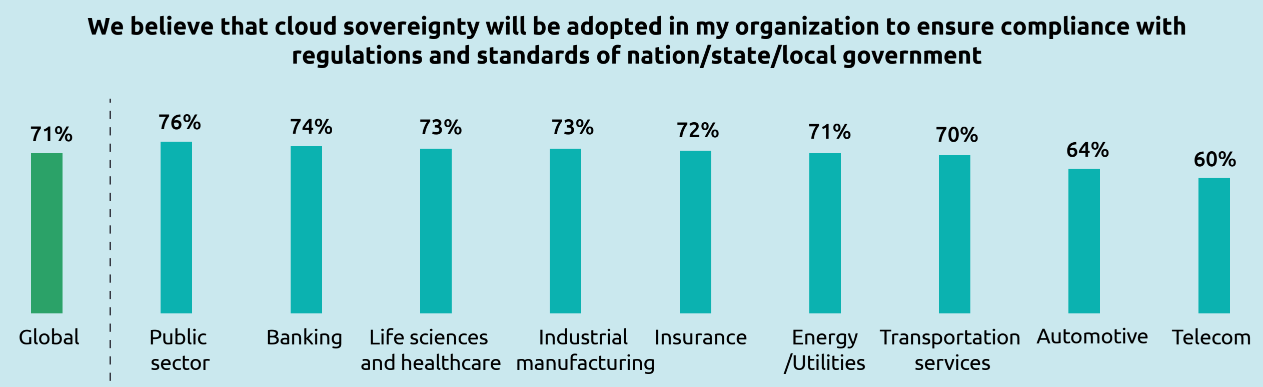
Regulatory drivers of cloud sovereignty by country and sector

Anne Perrin, ex-CEO Telefonica France & Northern Europe, explains, *"We do have clients coming for a sovereign cloud kind of setup, especially from the public sector. But most of the time, they would say it is for compliance and GDPR reasons that they need to be in Europe, or they need to make sure the data is in Europe as they cannot accept the Patriot Act implications. They don't use the particular words 'sovereign cloud,' as 'sovereign' can mean many things. They are going beyond the word 'sovereign' in security guidelines, in transparency guidelines, in data, and so on."*

Fig.8

Compliance with regulations is a key driver in countries such as Italy and Germany, and in certain sectors





Source: Capgemini Research Institute, Cloud Sovereignty Survey, May–June 2021, N = 1,000 organizations.

"We do have clients coming for a sovereign cloud kind of setup, especially from the public sector. But most of the time, they would say it is for compliance and GDPR reasons that they need to be in Europe, or they need to make sure the data is in Europe as they cannot accept the Patriot Act implications. They don't use the particular words 'sovereign cloud,' as 'sovereign' can mean many things. They are going beyond the word 'sovereign' in security guidelines, in transparency guidelines, in data, and so on."

Anne Perrin

ex-CEO Telefonica
France & Northern Europe

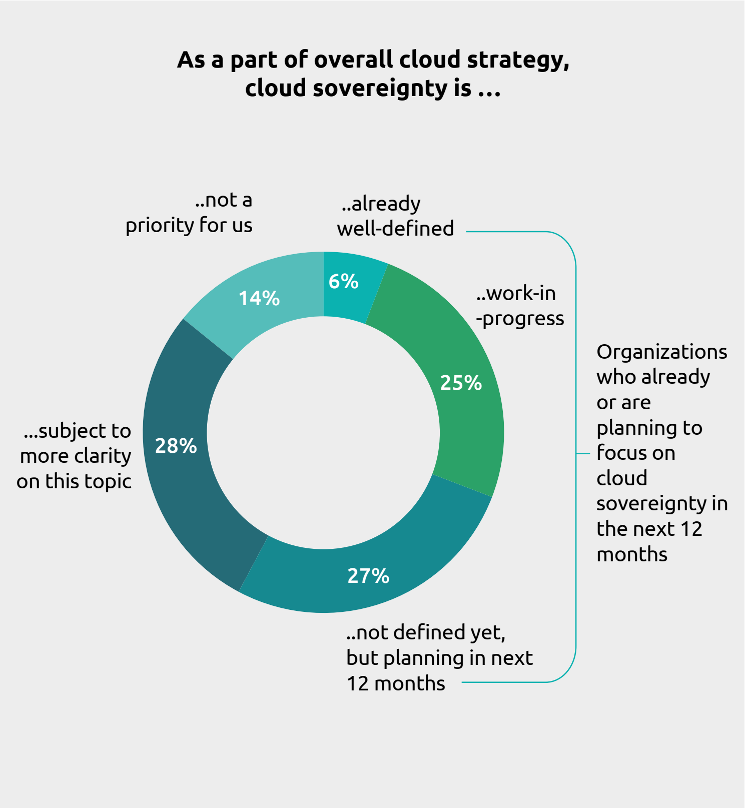
Organizations are actively investigating cloud sovereignty

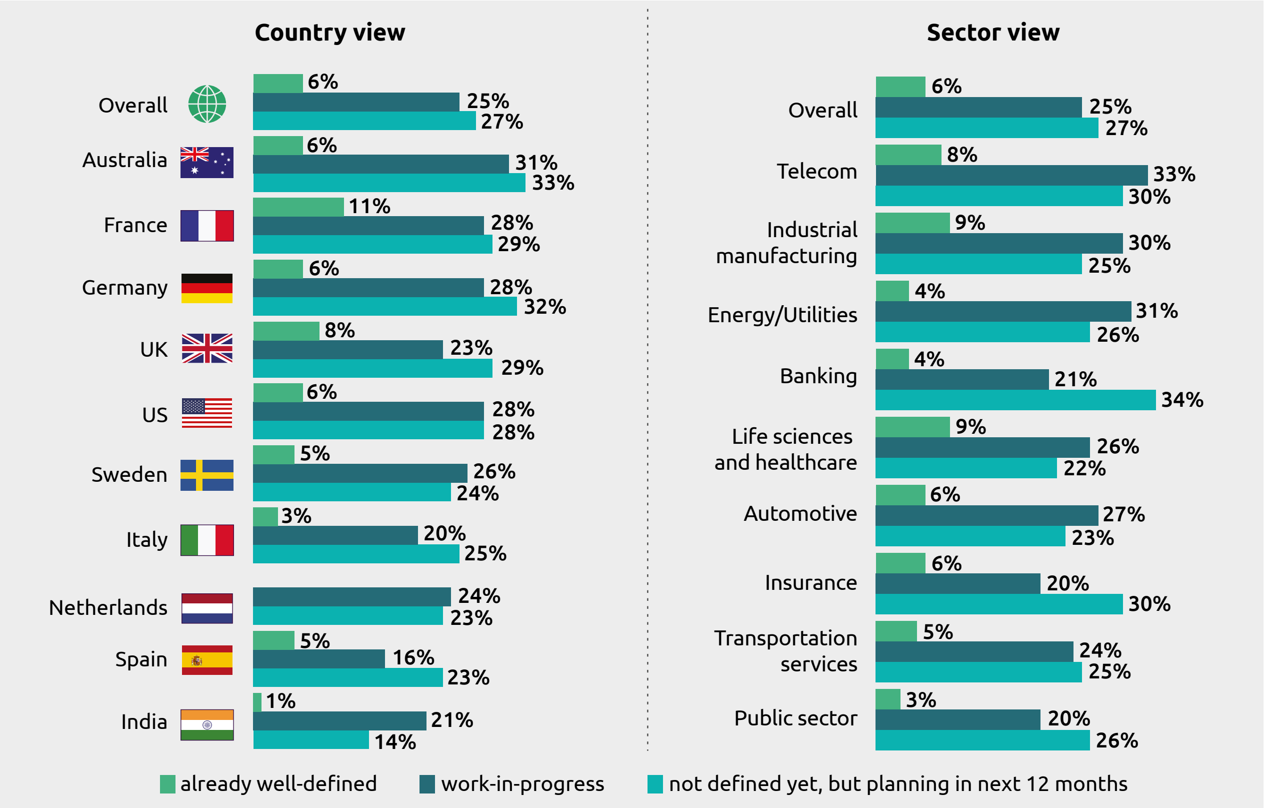
As a result of emerging regulations, laws, and discussions around cloud sovereignty, many organizations are making it a key consideration when formulating a cloud-adoption strategy. A senior executive from a European telecom company says, *"Migrating to cloud and organizing ourselves around public cloud is very much the priority for us. But I have to say that we are being cautious in our approach now, owing to the increasing importance of the sovereign cloud and the privacy aspect in Europe."*

- Nearly one-third (31%) of organizations are already embedding cloud sovereignty as a part of their overall cloud strategy, and 27% of organizations expect to start working on it in the next 12 months. Our research also found that nearly half (48%) of these organizations (for which cloud sovereignty is well defined, in progress, or planned in 12 months) already have most of their IT environment in the cloud today.
- Nearly 28% of organizations say that they need more clarity on this topic to form a cloud-sovereignty strategy, which highlights lingering uncertainty around sovereignty.

Fig.9

More than half of organizations will include sovereignty in their overall cloud strategies





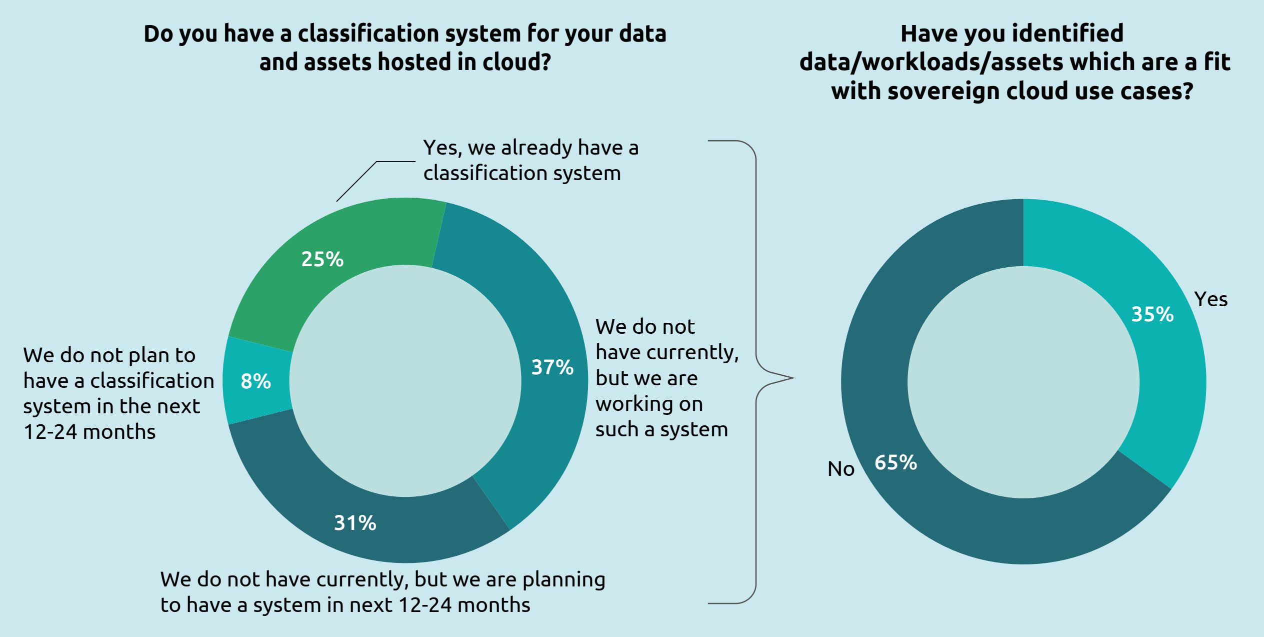
Source: Capgemini Research Institute, Cloud Sovereignty Survey, May–June 2021, N = 1,000 organizations.

Regulatory requirements also influence data and workloads planned in a sovereign cloud

Data classification helps organizations determine and assign relative values to their data, and to categorize their stored data by sensitivity and business impact to determine associated risks. Our research shows that, although only a minority (25%) of organizations currently have a classification system for data and assets hosted in the cloud, more than two-thirds (67%) are either working on it or plan to do so in the next 12–24 months. Of these organizations, more than one-third (35%) have already identified data, workloads, and assets that are a fit with sovereign cloud use cases.

Fig.10

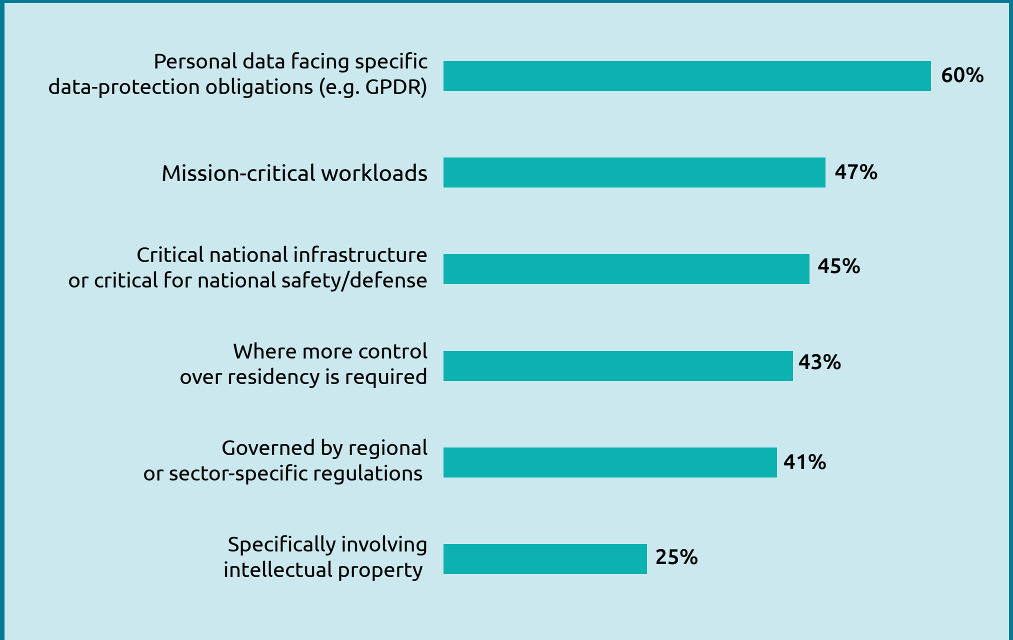
Organizations have started to identify data and assets fit for sovereign cloud



Source: Capgemini Research Institute, Cloud Sovereignty Survey, May–June 2021, N = 1,000 organizations (left-hand chart); N = 892 organizations that are planning to identify workloads for sovereign cloud (right-hand chart).

Fig.11

Workloads that organizations deem fit for sovereign cloud



Source: Capgemini Research Institute, Cloud Sovereignty Survey, May–June 2021, N = 314 organizations that have identified data/workloads/assets that are a fit with sovereign cloud use cases.

Unsurprisingly, these workloads are driven by regulatory factors, such as those containing personally identifiable information, those critical to national safety/defense, or those subject to controls (see Figure 11).

On mapping the workloads identified by organizations with our definition of cloud sovereignty (section 1, above), the workloads identified clearly relate more closely to "data sovereignty;" we investigate this more closely in the next section.

67%

organizations are either working on having a "classification system for data and assets hosted in the cloud" or plan to do so in the next 12-24 months.

Organizations are currently limiting cloud sovereignty to data localization

In our research, we asked more than 1,000 global organizations across sectors for their definitions of "cloud sovereignty":

- 43% of organizations focus on **data localization** (keeping the data within their preferred jurisdictions – usually within country/regional borders), irrespective of whether the public or private cloud provider is of local origin. This is more commonly the case with organizations in the energy/utilities (49%) and insurance (47%) sectors than in the public sector (39%).
- 14% define cloud sovereignty as exclusive use of cloud providers based in the same legal jurisdiction and storing data within country/regional borders.

A senior executive at a large US-based bank comments, *"Sovereignty, for me, means adhering to the law of the land in that particular region, primarily with respect to the data rules regarding customer data. The second part concerns transactions and where they should be stored. So, sovereignty for me is standing by the local law and adhering to the rules for data governance."*

Moreover, when asked about the expected cloud environment in the next 1–3 years:

- More than one-third (38%) expect to have a public or hybrid cloud environment where the vendor can be of local or non-local origin; but the data will reside within their country/region/jurisdiction's approved data centers. In France, 45% of organizations expect to focus on data localization, regardless of the nationality of the cloud service provider. From the sectorial view, 46% of industrial manufacturing and 45% of public services organizations agree with this.
- Globally, 16% of organizations expect to use a disconnected version of a hyperscaler and 14% prefer to work with the local legal entity of a hyperscaler.

- Only 11% say that they will be working exclusively with cloud providers based in the same legal jurisdictions as their organizations and adhering to data-localization requirements. It is interesting that 22% of organizations in the life sciences and healthcare sectors, and 14% in industrial manufacturing, say they will focus exclusively on local cloud providers. In terms of countries, this holds true for 15% of organizations in Germany.

It is interesting to observe that many organizations prefer data localization irrespective of the origin of the vendor in Figure 12 above. Key reasons for this include: organizations place importance on innovation and scale provided by global players today (see Figure 14, below); many are still awaiting greater clarity and guidance on regulations surrounding cloud sovereignty; they are also looking at their service providers for options on how to manage the sovereignty issues. Further, even on the supply front, cloud solutions with sovereignty-related factors are currently evolving and upcoming (see Figure 15). However, within organizations, the awareness of these options is also very low.

Fig.12

Organizations associate cloud sovereignty with data localization, irrespective of actual degree of sovereignty

	Public cloud with non-local origin vendors and without any restrictions of where cloud is being deployed, managed or governed	Public or hybrid cloud (including vendors of non-local origin); and data localization within national/ regional borders at locally–approved data centers	Use of disconnected or open source software platforms or components from vendors of non-local origin	Operation of non-local solutions by a trusted local provider or a local legal entity	Exclusive use of cloud providers based in the same legal jurisdiction and storing data within national/ regional borders	100% in-house private cloud
Expected Sovereignty Continuum*	**Least sovereign**					**Most sovereign**
What do organizations most associate with cloud sovereignty? (Top 1 ranked)**	0%	43%	8%	12%	14%	22%
What solutions are expected to be used in next 1–3 years?* **	16%	38%	16%	14%	11%	6%

*Note:*highlights expected continuum of cloud sovereignty – from blue (representing lesser degree of sovereignty) to green(representing greater degree of sovereignty); **highlights organizational definition of sovereignty; ***highlights expected solutions in the next 1–3 years*

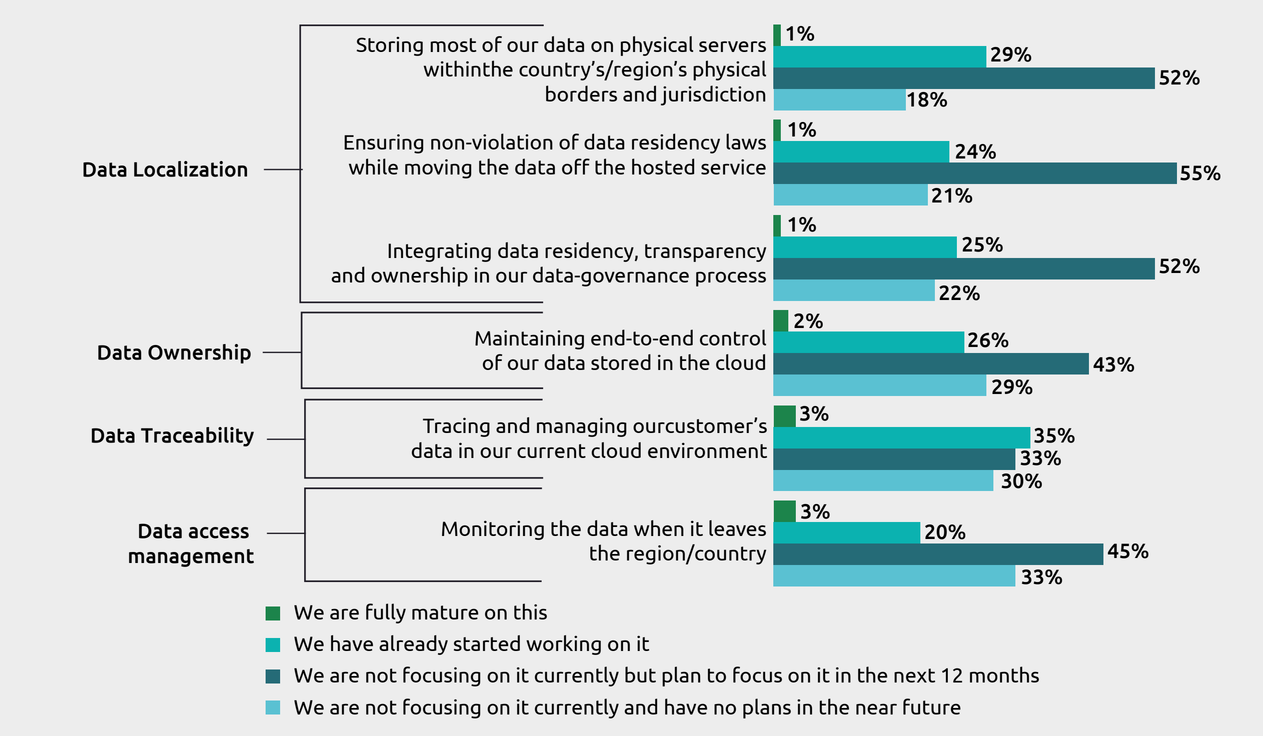
Source: Capgemini Research Institute, Cloud Sovereignty Survey, May–June 2021, N = 1,000 organizations.

At the same time, our findings raise pertinent questions about the complexities that may arise from data localization. For instance, how would clarity around governance be affected if the cloud service vendor and the data and applications of the organizations belonged to different jurisdictions? In such cases, which country should legislate on and govern the data and applications? As sovereignty-related regulations evolve in different geographies, will the sovereignty preferences of organizations expand beyond the current data localization? Further, should organizations have regional/country-specific cloud sovereignty strategies to host regional data? Are hardware and software sovereignty addressed?

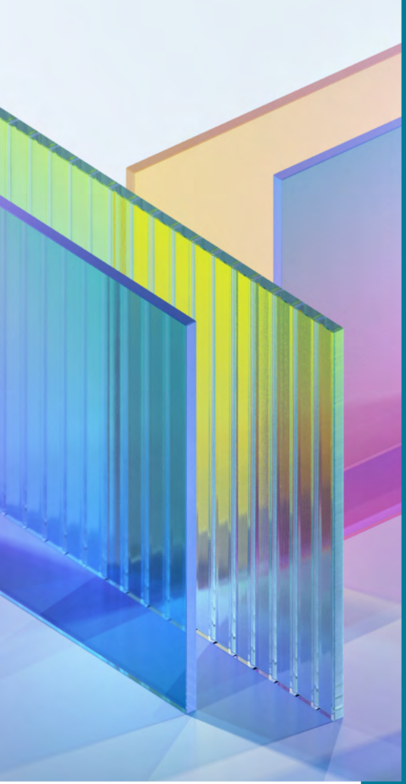
Data residency – a key focus area: Among other elements of cloud sovereignty (see definition in Figure 1), more than half of organizations point to "data residency" as a key area in the next 12 months (see Figure 13). A senior technology executive at Sydney Trains Australia says, *"Data residency is the most important aspect of sovereign cloud for us. With a SaaS, IaaS, or PaaS platform, it has to be in Australia and follow data sovereignty. As a public-transport provider for New South Wales, we need to follow the government guidelines for a critical infrastructure organization."*

Fig13

Various data residency "elements" are key priority areas for organizations in the next 12 months



Source: Capgemini Research Institute, Cloud Sovereignty Survey, May–June 2021, N = 1,000 organizations. Organizations were asked to rate their extent of preparedness for the above statements.

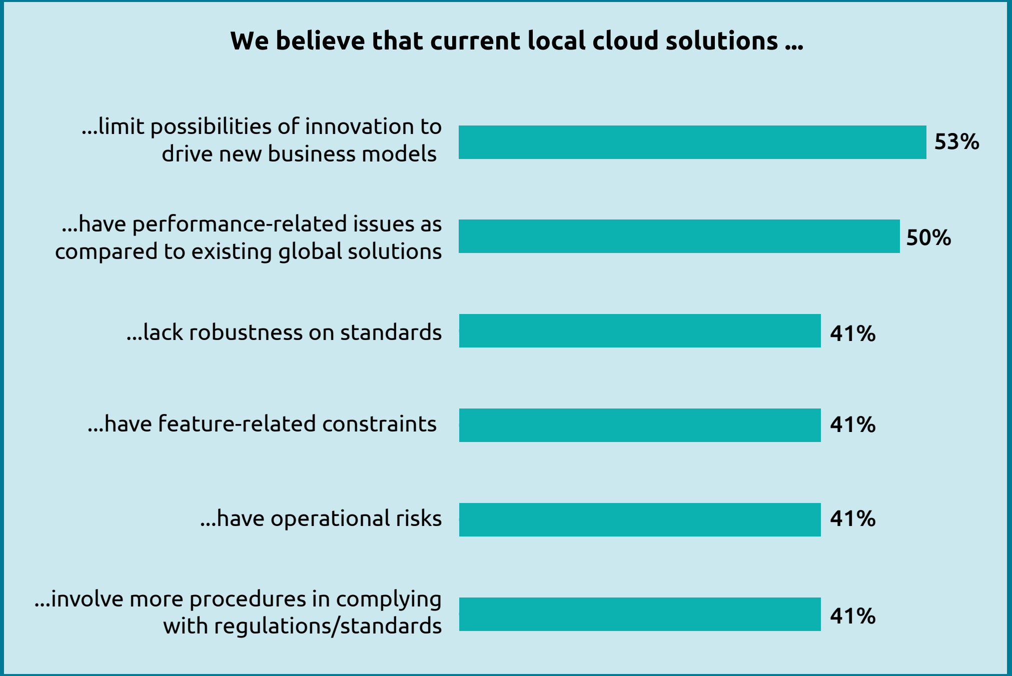


Half of organizations say local players don't match the innovation capabilities of hyperscalers

As Figure 12 shows, only 11% of organizations expect to work exclusively with local cloud providers within the next three years. We wanted to identify which perceived limitations were driving this trend. As Figure 14 shows, more than half of the surveyed organizations say that current local cloud offerings lack the innovation capabilities and speed of execution of global hyperscaler solutions. Beatrice Sablone, chief data officer at Arbetsförmedlingen (the Swedish public employment service) adds, *"There are major advantages that hyperscalers have over local CSPs or on premises – all the things you can do with the data; all the tools hyperscalers provide; the speed at which they discover threats and viruses and come up to with fixes and patches. You can never compete with that."* The concern about local providers' innovation capabilities is highest in Spain (63%), France, and the UK (both 57%).

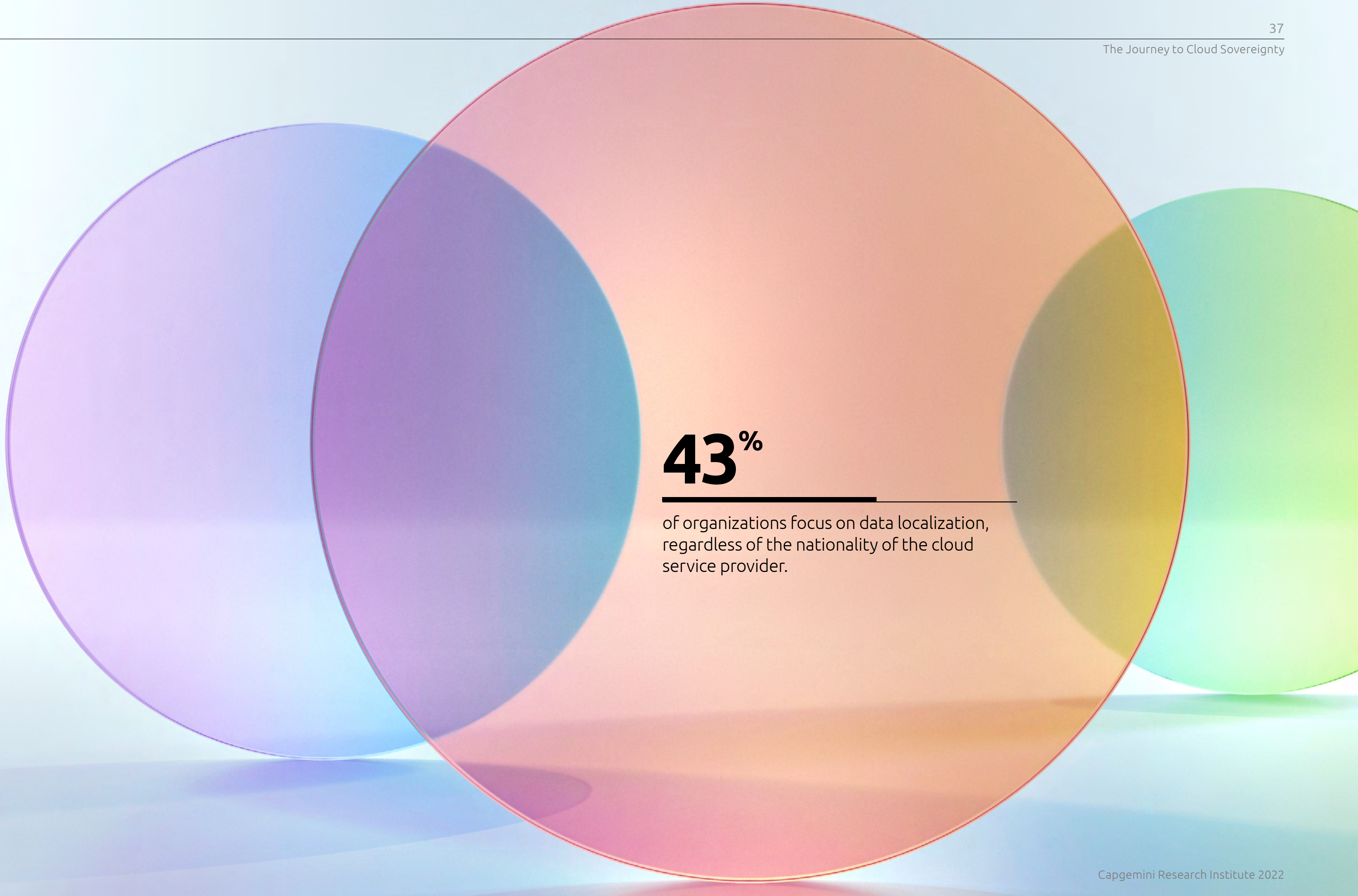
Fig.14

Organizations have concerns with existing local cloud solutions



Source: Capgemini Research Institute, Cloud Sovereignty Survey, May–June 2021, N = 1,000 organizations.

Note: Local cloud solutions are cloud offerings from service providers based in the same jurisdiction and storing data within the country's local data borders.



43%

of organizations focus on data localization, regardless of the nationality of the cloud service provider.

Cloud providers are establishing varying sovereignty offerings

As a response to the growing push on sovereignty – and to alleviate the concerns regarding loss of control over data – many cloud providers are already adapting their offerings to incorporate varying degrees of sovereignty while moving to the cloud. Some of the ways in which this goal is achieved includes:

Fig.15

Vendors are offering varying degrees of sovereignty solutions (indicative list)

Giving customers a choice in selecting where their data/ applications is hosted

- Salesforce, for instance, has stated that its platform can now be enabled on public-sector infrastructure across different countries. Enabling enterprises to host their data and applications at the location of their choice helps facilitate compliance with data protection and sovereignty laws.[27]
- Various ecosystem players are also catering to customer demand for storing sensitive data locally. For instance, NTT, the telecom and information and communications provider, is expanding its data-center footprint in the UK and has earmarked £500m for expansion projects. Florian Winkler, NTT global data centers division EMEA CEO, comments, *"We continue to expand to meet the demand from our clients for high-quality data-center space and to protect the growing volume of their sensitive data."* NTT also plans local/regional data-center expansion in countries such as India and Hong Kong, to meet the growing demand from businesses.[28,29]

Offering customers greater control in storing, managing, and accessing workloads

- The control features offered to customers by the Google Cloud platform include storing and managing encryption keys outside the cloud and authority to share access to the keys (based upon detailed justification).[30]
- In 2021, Microsoft announced that it will enable EU-based customers to process and store their data in the EU.[31]

Facilitating interoperability and allowing customers to manage multi-cloud and hybrid environments

- Microsoft's Azure Arc, designed for hybrid and multi-cloud environment management and governance, allows customers to control Kubernetes clusters deployed across different environments, including Azure, on premises, and even allows them to bring non-Azure cloud platforms into the Azure environment, affording them a unified view.[32]
- Likewise, Google Cloud added AI and Kubernetes cluster-management capabilities to their Anthos platform so that organizations can handle AI workloads close to their data.[33]
- In Europe, France's OVHcloud operates the continent's largest homegrown public cloud. IONOS is a major player in Germany. AU cloud in Australia is a local cloud vendor focused on the Australian government (federal, state, and local) and on critical national industry communities. Likewise, UKCloud provides cloud services exclusively to UK public-sector organizations.

Creation of open-source-based or disconnected solutions

- Google Cloud's Anthos platform allows organizations to build and manage applications across hybrid platforms, including their on-premises Google Cloud and peer platforms, such as Azure.[34]
- Amazon EKS Anywhere enables organizations to have cluster-management solutions on premises; AWS Outposts enables customers to bring AWS options on premises to run applications with low latency and to meet local data-processing requirements;[35] and Microsoft's Azure Stack hub gives access to Azure services on premises for an autonomous cloud in connected or disconnected versions.[36]
- These versions can be hosted in client environments in order to support multi-cloud capabilities, and may offer many or a limited set of subservices through being connected to the main cloud (e.g., AWS Cloud, Azure).

Hyperscaler stack operated in partnerships

- Recently, Capgemini and Orange announced the launch of their future joint venture "Bleu" to provide trusted cloud ("Cloud de Confiance") services to address the unique needs of the French State, public agencies, hospitals, regional authorities, Vital Importance Operators (OIVs) and Essential Service Operators (OSEs). Once established, and subject to regulatory approvals, Bleu will offer Microsoft technology, including collaboration and productivity solutions of Microsoft 365, and services available on the Microsoft Azure cloud platform.[37]
- Recently, Thales announced the creation of S3NS – a French company designed to offer performance, services, and applications of Google Cloud technology to public and private organizations in France. S3NS will be compliant with the requirements of the "Trusted Cloud" label of France's Information Systems Security Agency (ANSSI) in the frame of the French State strategy.[38]
- Microsoft Azure has been collaborating with local partner 21Vianet to bring cloud services to China, operating through exclusive cloud regions specific to the region.[39]

03

Organizations expect cloud sovereignty to build trust, foster collaboration, and accelerate the move to a data-sharing ecosystem

The previous section shows that although organizational definitions and levels of understanding of cloud sovereignty vary widely, organizations are focusing on data localization. They consider it key to retaining control over data, managing regulatory risk, adapting to different country/regional policy environments, avoiding fines and penalties, and managing reputational risk. However, our research also indicates that, beyond these concerns, organizations are looking at cloud sovereignty for various other benefits, including better collaboration, increased data sharing, and greater trust. Many organizations that are currently in an on-premises environment see it as an opportunity to reap the huge benefits that cloud offers.

42%

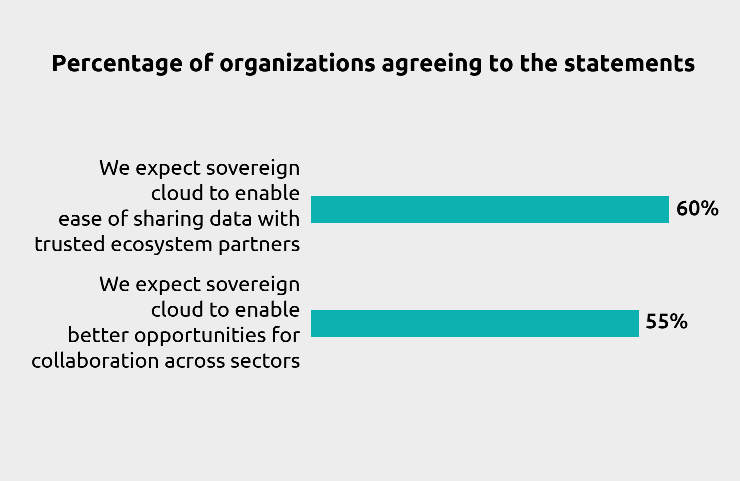
of executives believe that a trusted interoperable cloud service can help them to scale new technologies such as 5G, artificial intelligence (AI), and the internet of things (IoT)

Cloud sovereignty could offer collaboration and data-sharing opportunities with trusted ecosystem partners

With increasing digitalization and growing data ecosystems, collaboration, and data sharing within and across sectors has become increasingly important to organizational development. Our recent research revealed that, by engaging in data ecosystems, organizations have, on average, improved customer satisfaction by 15%; improved productivity/efficiency by 14%; and reduced costs by 11% annually in the last two to three years.[40]

Fig16

A majority of organizations expect that cloud sovereignty will make it easier to share data and collaborate with others



Source: Capgemini Research Institute, Cloud Sovereignty Survey, May–June 2021, N = 1,000 organizations. This includes share of respondents marking 5,6,7 to the above statements on a scale of 1 to 7 with 1 being Strongly disagree and 7 being Strongly agree.

Figure 16, above, shows a majority of organizations believe that cloud sovereignty will create better opportunities for collaboration across different sectors in a safe and secure manner. HPE's head of communication, Patrik Edlund, says, *"German car manufacturers are selling cars in France, for example, so they want their customers to be able to find a parking lot in Paris. They won't be able to do that if they only have data on their own fleet. They need all the data from Peugeot, from Citroën, and so on."*[41]

A few examples in this space are already emerging. For instance, IT services firm, Docaposte, life sciences major, AstraZeneca, and Impact Healthcare recently announced the creation of the Agoria Santé consortium, an organization that aims to bring together a collective of organizations in health and data science (hospital structures, academic players, pharmaceutical laboratories, medtechs, startups, etc.) The new entity would offer a sovereign platform for hosting and processing health data in research.[42]

It is also key to utilize the full potential of emerging technologies. In our research, 42% of executives believe that a trusted interoperable cloud service can help them to scale new technologies such as 5G, artificial intelligence (AI), and the internet of things (IoT). Dr. Michael Bolle, managing director, Robert Bosch GmbH, adds, *"From our point of view, data sovereignty and open exchange of data is a key success factor for new technologies such as machine learning, artificial intelligence, or the internet of things."*[43]

Cloud sovereignty could offer control and a trusted environment for data

Our research shows that 63% of organizations believe that cloud sovereignty will provide them with a trusted and secure cloud environment for data. The element of trust also opens up new possibilities of collaboration. More than half believe that cloud sovereignty provides better control over their own data and algorithms (see Figure 17). Hannes Kühn, deputy head of secretariat at National Regulatory Control Council Germany, says, *"Better data control, better service, data-access protection and compliance are the key benefits organizations can achieve by adopting sovereign cloud."*

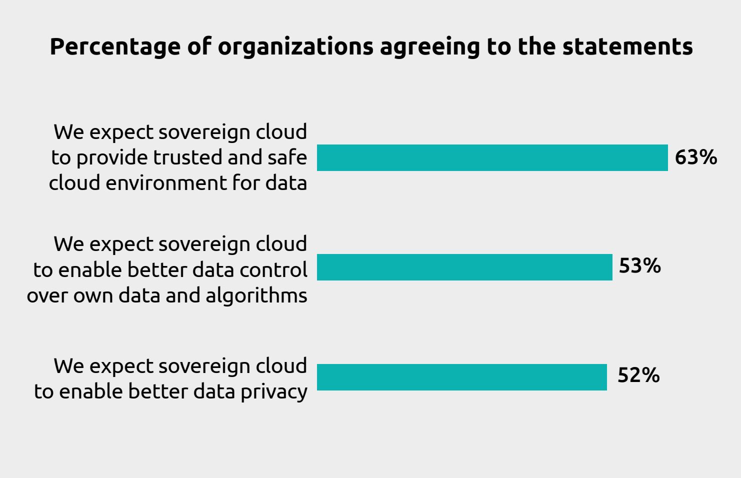
A majority of respondents in countries such as Italy, Netherlands, and Spain share this belief. And, by sector, most organizations in industrial manufacturing, telecoms, and the public sector agree as well.

63%

of organizations believe that cloud sovereignty will provide them with a trusted and secure cloud environment for data.

Fig.17

Organizations anticipate greater control and trust-related benefits from cloud sovereignty



Source: Capgemini Research Institute, Cloud Sovereignty Survey, May-June 2021, N = 1,000 organizations. This includes share of respondents marking 5,6,7 to the above statements on a scale of 1 to 7 with 1 being Strongly disagree and 7 being Strongly agree.

Cloud sovereignty in the public sector

A large majority of public-sector firms have concerns about public cloud

The public sector is undergoing digital transformation but remains apprehensive about including the public cloud as the core of these transformation projects. The major reasons for this are the sensitivity of the data involved and the lack of transparency from the cloud service providers in handling the data. This is also evident from our research results:

70% of public-sector firms are concerned about operational dependency on vendors based outside of their region's jurisdiction

69% of them are concerned about lack of transparency and control over what is done with their data in cloud

In addition to regulatory compliance, immunity from foreign access is a key driver for exploring sovereign – cloud solutions

Our research results also show that public-sector organizations are more commonly expected to trust and adopt the sovereign cloud than are organizations in other sectors:

76% of public-sector organizations believe that sovereign cloud will be adopted to ensure compliance with regulations and standards of the nation/state/local government

69% of them believe that sovereign cloud will be adopted to ensure immunity from extra-territorial laws

68% of them consider adapting to a country's policy environment to be a key driver of cloud sovereignty

Nearly half (48%) of public-sector organizations are either already considering cloud sovereignty as a part of their cloud strategy or planning to include the same in the next 12 months. Moreover, 57% of public-sector organizations believe that initiatives that prioritize sovereign cloud will become stronger in the next 12–24 months.

Public sector seeks greater trust as well as collaboration-related benefits from sovereign cloud

The public sector is also expecting more data-related benefits from sovereign cloud, which will allow it to store sensitive data in a secure and legally compliant public cloud, along with the benefits of innovation and scalability:

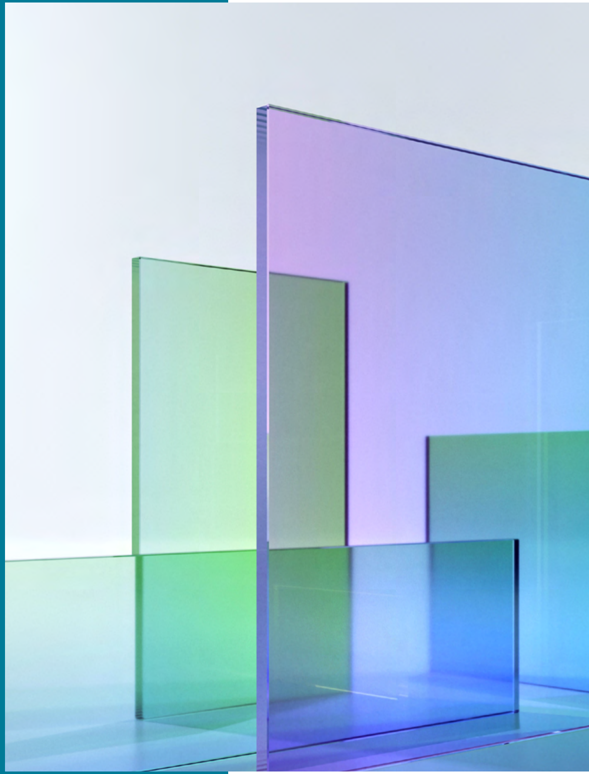
68%

of public-sector organizations believe that sovereign cloud will provide a trusted and secure cloud environment for data compared to **63%** from all sectors combined

59%

of them believe that sovereign cloud will provide better opportunities for collaboration across sectors as compared to **55%** from all sectors combined

Source: Capgemini Research Institute, Cloud Sovereignty Survey, May–June 2021, N = 1,000 organizations, N = 201 public-sector organizations.



Organizations will accelerate use cases as cloud sovereignty matures

In our research, we wanted to identify the most viable use cases for sovereign cloud. We looked at more than 50 use cases across ten sectors and, based on the survey as well as in-depth interviews, we identified more than 20 use cases, any of which could constitute a good starting point for organizations – both in terms of ease of implementation and upside benefit. More than one-third of organizations say that they do plan to pilot/test one or more of these use cases in the next 12–24 months. These use cases are not exclusive to sovereign cloud but are laid down by survey participants as the use cases they see as the most viable with which to start their sovereign cloud journeys.

Public sector:

In the public sector, sovereign cloud offers a variety of use cases, from smart cities to fraud detection. Our analysis highlights the following use cases:

Potential use case	Details	Percentage of organizations expecting *"high ease of implementation"* in this use case on sovereign cloud	Percentage of organizations expecting "high benefits" in this use case on sovereign cloud	Organizational priorities
Smart city services	Connecting data infrastructure in areas such as mobility, health, administration, energy and education, etc.	69%	62%	Nearly a third (30%) of public–sector organizations plan to implement **"fraud, error, and compliance"** in a sovereign cloud setup; 16% say they are already doing this.
Data-driven government	Usage of cross-department data	58%	61%	
Fraud and compliance	Fraud, error, and compliance detection for public sector	49%	45%	
Chatbots for digital public administration	24/7 digital assistance for citizens through chatbots	62%	61%	

Healthcare:

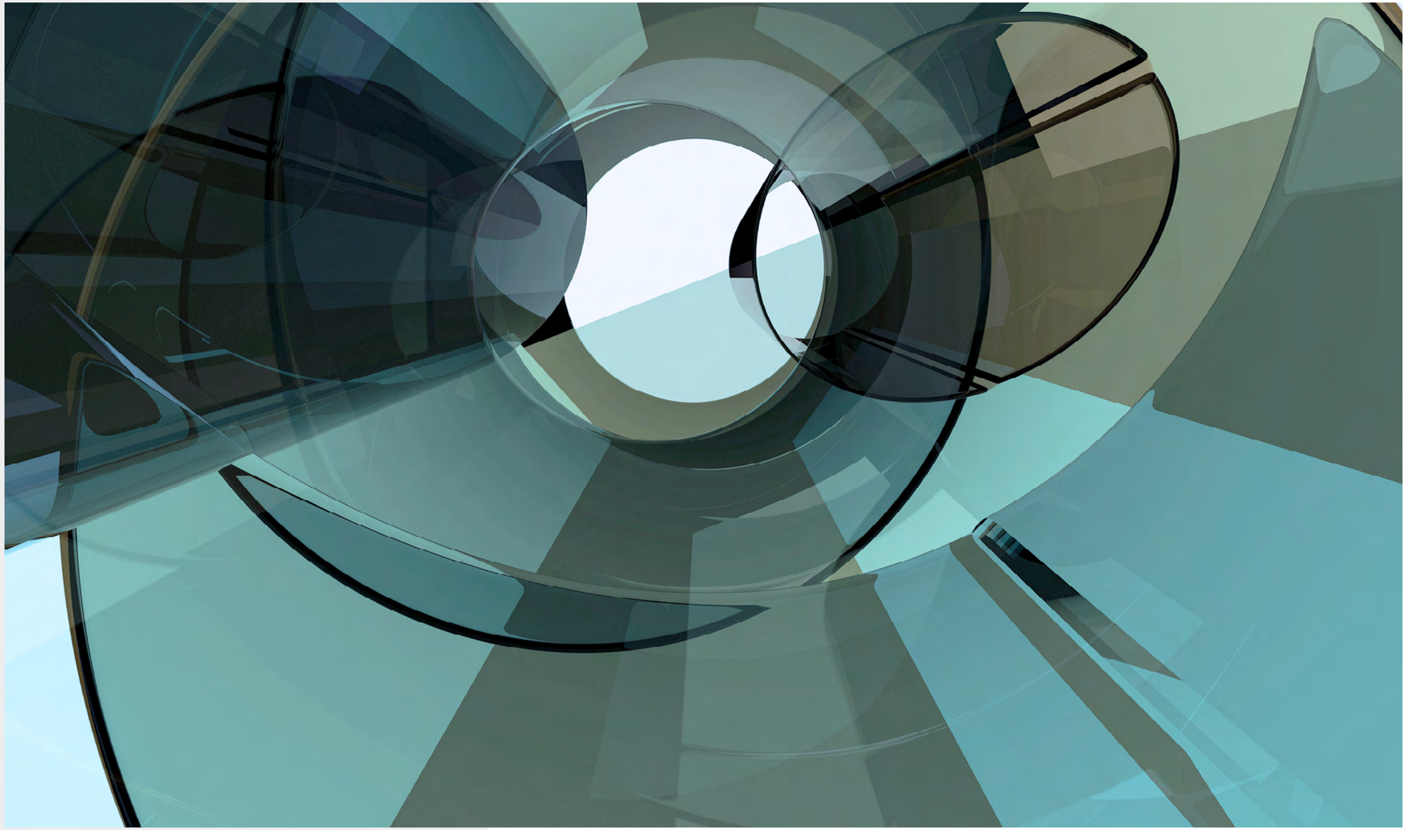
AstraZeneca's Christophe Dufour says, *"Medical analysis involving information around the management of a disease in real life – including understanding the pathology and the patient pathway – is the most appropriate use case for sovereign cloud in the healthcare sector. It is in the production phase currently at AstraZeneca."* Our own analysis shares this focus:

Potential use case	**Details**	**Percentage of organizations expecting *"high ease of implementation"* in this use case on sovereign cloud**	**Percentage of organizations expecting "high benefits" in this use case on sovereign cloud**	**Organizational priorities**
Remote patient monitoring	Remote patient monitoring for elderly citizens	70%	62%	Nearly 38% of healthcare and life sciences organizations are planning to test/implement **"integrated health platforms"** and 37% are planning to test/ implement **"digitized health"** records in a sovereign cloud set-up.
Healthcare platforms	Creation of healthcare platform and integrating patients with providers (e.g., hospitals, care services)	67%	68%	
Digitization of health records	Digitization of health records and providing access and control to patients about their health data	66%	67%	
Bio-medical research	(E.g. advanced areas such as genome sequencing, cancer research) through cloud	62%	61%	

Financial services:

A senior executive of a large US-based bank comments, *Sovereign cloud is going to be a big opportunity area for the banking industry and is going to be one of the important aspects of its cloud roadmap."* More than a dozen European financial institutions are coming together to drive forward public cloud adoption in a safe, secure, and controlled manner. They have jointly launched the European Cloud User Coalition (ECUC), which aims to "strengthen the public cloud ecosystem for the entire European financial industry."[44] The following use cases emerged from our research:

Potential use case	**Details**	**Percentage of organizations expecting *"high ease of implementation"* in this use case on sovereign cloud**	**Percentage of organizations expecting "high benefits" in this use case on sovereign cloud**	**Organizational priorities**
Seamless payments	Integrating card data, payment data of customers, digital wallets, etc., to facilitate seamless transactions	72%	71%	**43%** of financial-services organizations plan to implement **"authentication"** in a sovereign set-up in the next 12–24 months, whereas **9%** of organizations are already testing/ implementing this use case in a sovereign setup
Collaboration-led data platforms	Collaboration-led data platforms across firms integrating customer data, payments data	70%	65%	
Authentication	Using facial, voice recognition, biometrics on banking/ insurance platforms for authentication and identity management of customers	68%	63%	
Money-laundering detection	Detection of money laundering and fraud across the network	62%	61%	



Transportation:

Data sharing is an emerging use case for sovereign cloud in the transportation and mobility sectors. The ability to share data within applicable regulatory frameworks can reduce service delivery times, improve the customer experience, and help identify new revenue streams. For instance, the mobility working group at GAIA-X – including Air France-KLM, Amadeus SAS, Schiphol, and the Paris airports – is working on sharing passenger details between airlines, travel reservation systems, and airports. The aim is to eliminate the requirement to carry passports and enable travelers to navigate through airports more quickly. This data could be combined with COVID-19 vaccination data to ensure that travelers who have been immunized are not subject to quarantines or testing.[45]

Industrial manufacturing:

At Cornerstone Building Brands, a leading provider of exterior commercial and residential building products, Gordon Schembri, senior director, transformation and innovation, says, *"Design and structural drawings are one of the use cases from our industry that can be implemented in a sovereign cloud setup. For example, if we are working on an aircraft hangar, the structural designs for these hangars are large and confidential. At present, this kind of data is kept nearly 90% on premises. But, in a sovereign cloud setup, we can have this data closely monitored in a location where we want it to reside, with the controls and mechanisms we want. This use case is in the proof-of-concept stage in our company."* Our research identified the following:

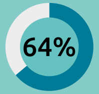
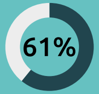
Potential use case	Details	Percentage of organizations expecting *"high ease of implementation"* in this use case on sovereign cloud	Percentage of organizations expecting "high benefits" in this use case on sovereign cloud	Organizational priorities
Data exchange	Cross-company collaborations on data exchange to generate new business models (ex. shared production)	68%	61%	41% of industrial manufacturing organizations plan to test/implement **"data exchange for new business models"** in a sovereign setup. Nearly 17% are already testing/implementing this approach.
Collaborative real-time monitoring	Collaborative real-time monitoring of industrial plants involving aggregation of data across the network involved, such as component manufacturer, machine manufacturer, production data, etc.	58%	53%	

A senior executive at a US-based automotive organization says, *"Automobile manufacturers like us have different blueprints and different manufacturing processes, designed by automobile engineers, which guide the production of our vehicles. So, I think all the information that's housed in terms of our data and our trade secrets in our collaboration with other companies, any collaborative documents, or I would sum up by saying our product-development processes along with 3D printing and AI tools used in manufacturing, would be important use cases for sovereign cloud."*

Another prominent use case for manufacturing is digital supply chains – which includes the integration of data information across the supply chain including component manufacturers, machine operators and maintenance service providers. All the stakeholders benefit from a secured information exchange that can be regulated from a shared cloud environment.

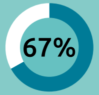
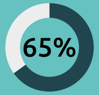
Energy and utilities:

In critical national infrastructure (CNI) industries, such as energy and utilities, the data generated by systems could be used to perform preventive maintenance. With a sovereign cloud, data can also be shared with the wider ecosystem and can be incorporated with peer data without it being shared publicly.

Potential use case	Details	Percentage of organizations expecting *"high ease of implementation"* in this use case on sovereign cloud	Percentage of organizations expecting "high benefits" in this use case on sovereign cloud	Organizational priorities
Data exchange across energy sector value chain	Data exchange/coupling among sectors (e.g., data exchange among energy and mobility sectors for EV forecast models)			**39%** of energy and utilities organizations see a case for testing **"data exchange"** in a sovereign cloud set-up

Telecom:

Our research shows that telecom organizations are focusing on network management as a prominent use case in a sovereign cloud setup.

Potential use case	Details	Percentage of organizations expecting *"high ease of implementation"* in this use case on sovereign cloud	Percentage of organizations expecting "high benefits" in this use case on sovereign cloud	Organizational priorities
Network management	Monitoring and managing network-related data			**35%** of telcos plan to test/ implement **"network management"** in a sovereign cloud setup

04

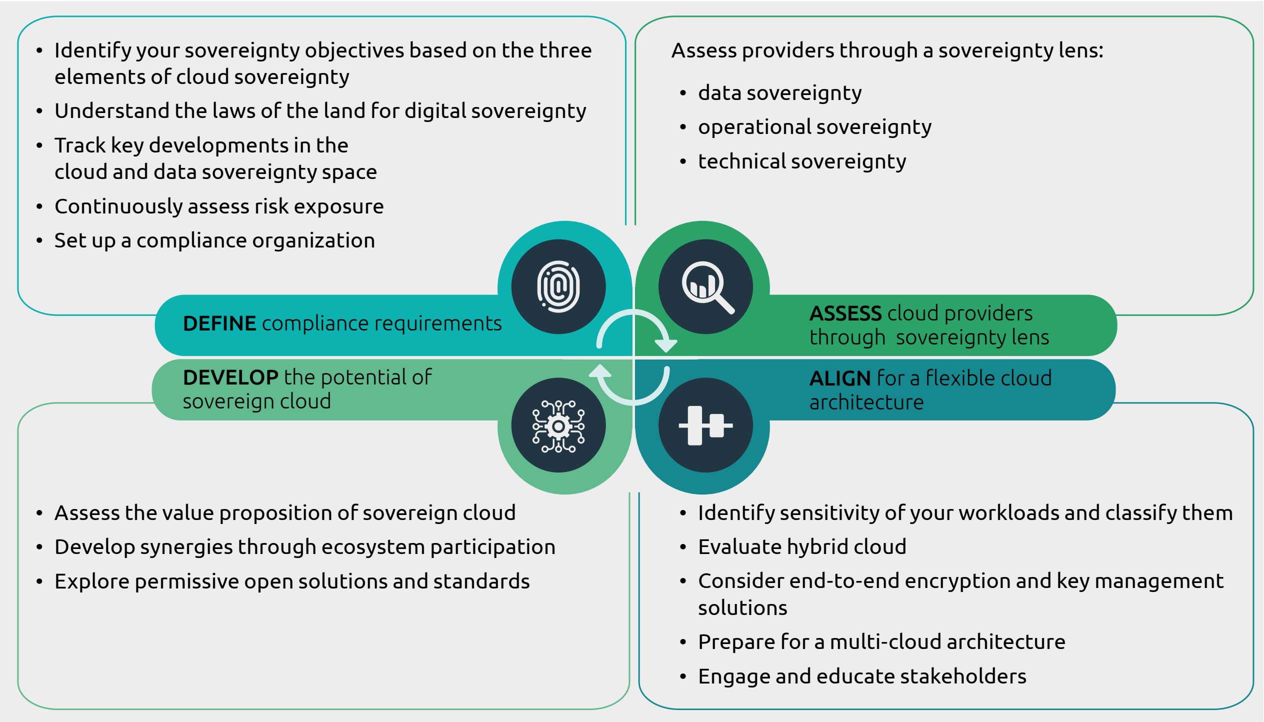
How can organizations build their “move-to-sovereign” strategies?

As highlighted in section two, the definition of cloud sovereignty varies between organizations. Many organizations are concerned about the presence of extra-territorial laws but, at the same time, they are keen to utilize the innovation, breadth of capabilities, and scale offered by the cloud providers. With the cloud sovereignty space fast emerging, organizations need to stay ahead of the curve – from understanding the emerging trends, to factoring elements of sovereignty into the overall cloud strategy, as well as ensuring technical flexibility in their cloud architecture.

In this section, we outline four key recommendations for organizations to focus on in their move-to-sovereign strategies (see Figure 18). These recommendations can help organizations in understanding the areas of focus when embedding cloud sovereignty in their overall cloud strategies:

Fig.18

Four key pillars for a "move-to-sovereign" strategy



- Identify your sovereignty objectives based on the three elements of cloud sovereignty
- Understand the laws of the land for digital sovereignty
- Track key developments in the cloud and data sovereignty space
- Continuously assess risk exposure
- Set up a compliance organization

DEFINE compliance requirements

Assess providers through a sovereignty lens:

- data sovereignty
- operational sovereignty
- technical sovereignty

ASSESS cloud providers through sovereignty lens

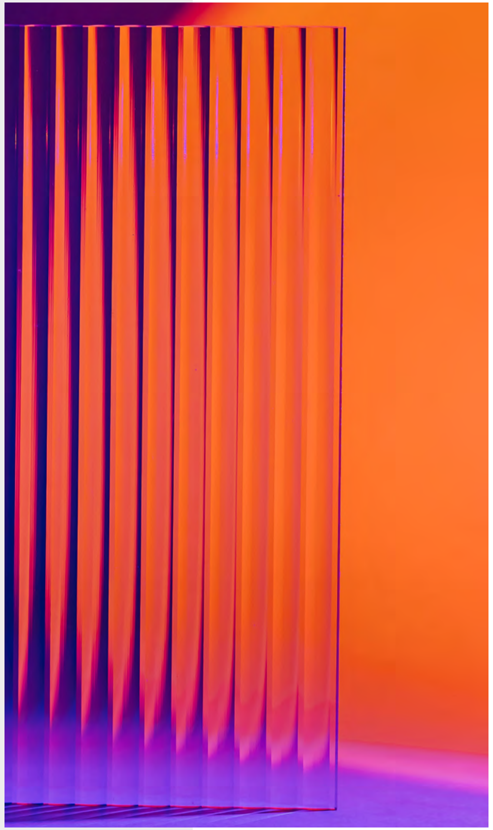
DEVELOP the potential of sovereign cloud

- Assess the value proposition of sovereign cloud
- Develop synergies through ecosystem participation
- Explore permissive open solutions and standards

ALIGN for a flexible cloud architecture

- Identify sensitivity of your workloads and classify them
- Evaluate hybrid cloud
- Consider end-to-end encryption and key management solutions
- Prepare for a multi-cloud architecture
- Engage and educate stakeholders

Source: Capgemini Research Institute Analysis.



DEFINE compliance requirements

Sovereignty becomes clear when cloud is hosted privately or using on-premises infrastructure. With the growing popularity of public cloud, organizations are likely to prefer hosting their cloud in regions closer to end users, aiming for an improved user experience, cost efficiencies, and reduced latency. In cases such as these, organizations need to be aware of the sovereignty requirements on their cloud infrastructure from different perspectives. They need to:

Identify sovereignty objectives:

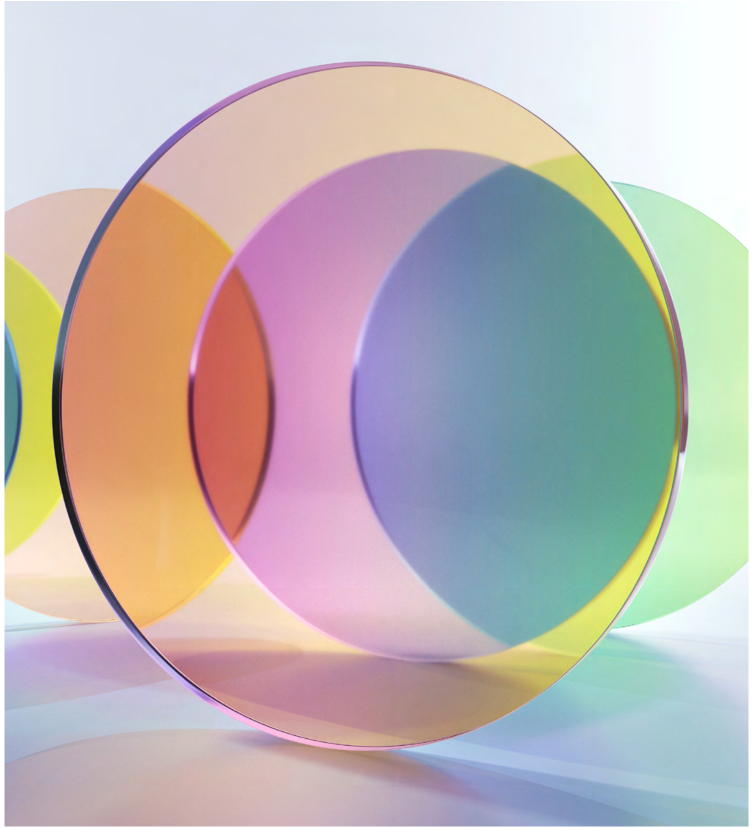
Identifying your sovereignty objective is the first key step for organizations. Is your objective to a keep a tighter control of your data? Or is it about preventing unsolicited third-party access? Are you aiming to focus more on regulatory compliance or is it about running workloads without continuous dependence on a provider's cloud?

Our framework referring to three elements of cloud sovereignty: data sovereignty, operational sovereignty, and technical sovereignty can help organizations to define their objectives in the first place.

Understand the laws of the land for digital sovereignty:

Organizations need to be aware of the compliance requirements mandated by their country and applicable to their sector to prevent compliance violations.

- Take the UK's health-service technology organization, NHS Digital. Its guidance for public cloud use states that the country's NHS and social-care providers can store confidential patient data in a public cloud, as long as it is hosted within the UK or European Economic Area (EEA). The initial guideline stated that it can also be stored in the US, where it is covered by the privacy shield, but, in light of the annulment of the privacy shield, the guidelines need to be revisited.[46]
- Similarly, in the US, those healthcare organizations using cloud are required to comply with the country's Health Insurance Portability and Accountability Act (HIPAA) to ensure security and privacy of health records. [47]
- The French government has declared that its most sensitive state and corporate data can be stored by Google and Microsoft using their cloud-computing technology if it is licensed to French companies. The servers need to be located on the French soil and European ownership of the companies storing and processing the data need to be guaranteed.[48]



Failure to understand and follow these data-residency requirements raises the risk of wasted resources in the form of staff time and technical investments or even fines for violating regulations such as the GDPR.

Along with understanding the data laws of their primary national governments, organizations also need to keep track of overseas laws if their public cloud infrastructure is hosted there. In the US, this can mean understanding both federal law and state law. For instance, if the business is based in the US, and has a public cloud server in California, then they may be subject to the state-specific California Consumer Protection Act (CCPA), as well as federal laws.

Track key developments in the cloud and data sovereignty space:

For instance, since digital sovereignty has become a hot topic for European organizations and governments, they must keep an eye on developments such as GAIA-X. Arbetsförmedlingen's Beatrice Sablone adds, *"Sovereign cloud would be like a cloud that abides with the area's laws 100% and is restricted to that area. In Europe, GAIA-X is trying to become that technology set, along with rules and regulations, but it's not a physical cloud. I would say, if you want to have an EU cloud, you should follow the developments within GAIA-X."*

Organizations should:

- Check alignment of these initiatives with their business goals
- Nominate a representative to track the progress of these initiatives
- Participate in working groups to understand institutional standards and highlight key end-user needs.

Continuously assess risk exposure:

Organizations need to understand the risk implications of being subject to foreign regulations (for example, if a data center is located overseas). The Bank of England, for instance, is currently working with the UK Treasury and the Financial Conduct Authority (FCA) to assess the different risks (such as concentrating risks in a particular country) that result from banks' moving sensitive applications to the cloud, especially when it is with non-local providers.[49]

Further, given that the regulatory environment changes so quickly and often, it is critical that due diligence on sovereignty requirements is conducted on an ongoing basis.

"Sovereign cloud would be like a cloud that abides with the area's laws 100% and is restricted to that area. In Europe, GAIA-X is trying to become that technology set, along with rules and regulations."

Beatrice Sablone

Chief data officer at Arbetsförmedlingen (the Swedish public employment service)

A senior technology executive from Sydney Trains Australia adds, *"To the companies that are moving to sovereign cloud, I would recommend making sure that you have clear governance and policy. Make sure that you are following the guidelines and policy that you have either created or you are inheriting from your overall authority, whether it's federal government, local government, or your sector's governing body. Have that protection in place, and then make sure that those protections and guardrails are built into the environment so that they allow staff to be able to go and play without the risk of making mistakes."He emphasizes the importance of these "guardrails," as well as technical controls, specifically when relying on out-of-region players.*

Set up a compliance organization:

As the sovereignty landscape evolves, setting up a compliance organization and establishing processes will be key. Organizations will need to document their processes and be ready to produce that documentation to prove cloud and data-sovereignty compliance. Committing to a comprehensive compliance program, addressing budget requirements, regular audits, legal-policy reviews, and updates and awareness-related programs will be critical.

This will also call for an expansion of the role of chief data protection officer, as well as establishing a network of data protection officers throughout the organization. These data protection officers will ensure that data sovereignty is maintained, and that it follows the laws of the country where data is physically stored. This network needs to be defined in accordance with the company's structure and organization, in order to ensure effective representation throughout the business units and legal entities of the company.

ASSESS providers through a sovereignty lens

Telefonica's Anne Perrin says,*"'Sovereign' doesn't mean national or European, it means guided by rules that we in Europe feel comfortable with and that our customers feel comfortable with. It's about elements such as transparency, being able to tell customers where the data is; how it's stored; what security policies surround it; where the value goes; who owns the solution; and how to split responsibilities between the partners."* While guidelines regarding cloud sovereignty are still evolving, we have compiled a key transparency and controls-related indicative checklist to be considered when assessing global or local vendors from the perspective of sovereignty – Data, Operational, and Technical. Organizations also need to conduct an application, data discovery, and data-protection impact assessment, as well as formulate an app, data, and cloud-migration strategy.

Data sovereignty:

- **Data residency, control, and transparency:**
  - – Do you control the location of your data?
  - – Does the vendor offer regional and localized data centers as approved by the local government? Do they have tie-ups with trusted local providers to offer data localization and is that permissible under local guidelines and regulations?
  - – Do they have transparent policies on data geolocation (for instance, giving firms tools to identify and track the location of the data)?
  - – Do you maintain the end-to-end control of your data stored in cloud?
  - – Do you have visibility and control over your vendor's administrative access to data?
  - – Do you have technical controls to block asset creation or data transfer out of the region?
- **Storage and back-up:**
  - – Where are the back-ups, imaging, and archived versions of the data and applications kept, and are the organizations made aware of it?
  - – Are you able to audit your vendor periodically?

Operational sovereignty:

- **Security and compliance:** Our research shows that, for 71% of organizations, cloud service providers' compliance with national cybersecurity standards and certifications is a key focus area. Paul König, VP – head of IT at Bavaria State Tax Office, Germany says, *We are already looking at what could be there in the cloud – for us, sovereign public cloud is a quite conceivable option. A key requirement is that data security must be fulfilled."*

  Key aspects to consider include:
  - – Does the vendor have the required national and international security certifications?
  - – How effective is the protection from unintended access?
  - – Can you view security configuration changes to infrastructure and hardware?
  - – Has the sovereignty of applications and application-management tools been addressed?

"We are already looking at what couldbe there in the cloud – for us, sovereign public cloud is a quite conceivable option. A key requirement is that data security must be fulfilled."

Paul König

VP – head of IT at
Bavaria State Tax Office,
Germany

- **Operational resilience:**
  - Does your vendor provide local support and administration within selected regions?
  - Does your vendor ensure continuity of cloud service in the event of international uncertainties or disruptions?
  - Does your vendor have control over the technology powering the cloud?
  - Do they account for outages and incidents in the design of the cloud itself?
  - How do they account for the impact of regulatory changes?

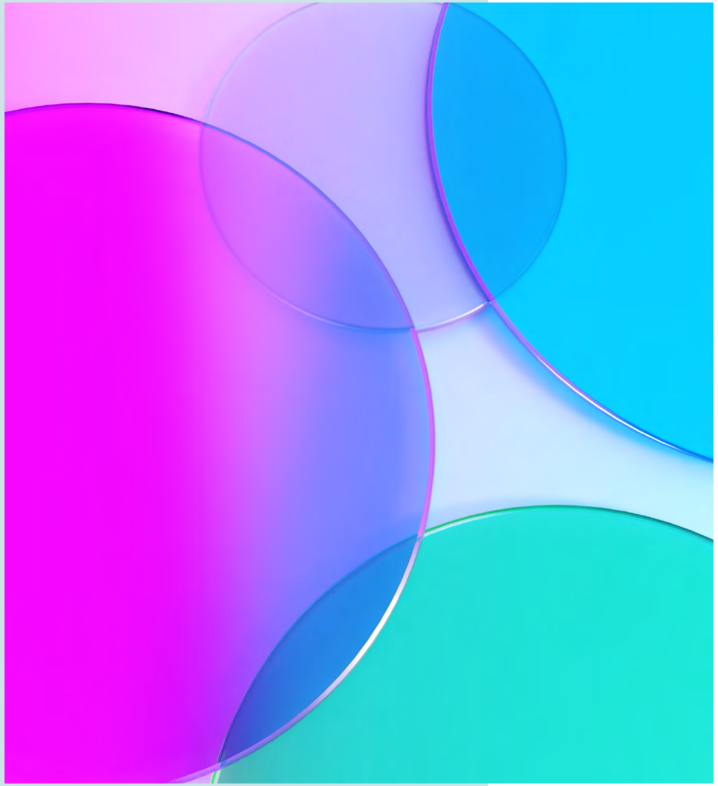
Apart from these, it is also crucial to understand the sovereignty of the ecosystem, which involves cloud providers, telcos, application programming interfaces (APIs), etc.

Technical sovereignty:

Christophe Dufour, chief digital officer at AstraZeneca France, says, "*The local cloud provider also needs to provide interoperability. We ask our local provider to use standard solutions. For example, we use some very common solutions coming from other countries such as containers. As a customer, it's really important for me that a sovereign cloud provider can give me the same interfaces and the same components as the other provider. Interoperability is very, very important to me as a customer."*

Key issues include:

- Are there intuitive interoperability and migration features with other cloud solutions that you use?
  - On that note, a few countries are also mandating data portability and interoperability as a precursor to moving to cloud. For instance, the European Union Agency for Cybersecurity (ENISA) has proposed cloud guidelines for healthcare organizations that require data portability and interoperability as part of their security requirements, in addition to data encryption and incident-management processes.[50]
- Do you have a clear exit policy/process in collaboration with your cloud vendor?
- Are you keeping your business rules separate from your software solution?



ALIGN for a flexible cloud architecture

Identify sensitivity of the workloads and classify them:

Certain data points – such as customer or citizen data, or data that contains personally identifiable information (PII) – are sensitive. Usually, therefore, they are protected by regulations such as the GDPR. To avoid compliance violations, organizations need to review and classify their data and check it fits with sovereign use cases. As mentioned previously, currently only a minority (25%) of organizations have implemented a classification system for data and assets hosted in the cloud, and an even smaller minority have identified the data, workloads, and assets that are a fit with sovereign cloud use cases. As mentioned in the previous section, a strategy to identify the first use cases of sovereign cloud will also be key.

Organizations need to:

- Be aware of the types of data that are hosted in the cloud and the importance of different data types for the organization
- Consult with in-house, as well as external, security professionals about the legal interpretation of such data
- Identify requirements for user's rights, access management and role-based authentication requirements
- Perform regular data-protection impact assessments to safeguard sensitive data in public clouds

Evaluate hybrid cloud:

As an alternative to pure "hyperscaler vs local" cloud selection, organizations should consider whether a hybrid solution would cater more closely to their needs. In other words, a sovereign solution for the most sensitive data, applications, and workloads, and a global solution for less sensitive ones.

"The encryption of data can be a potential alternative to sovereignty in special cases. Of course, this requires more calculation power and sometimes takes away usability, but it's an option, or it's even mandatory when we are really sharing or transporting data from A to B. But that's only one of the solutions we have to look into, while we will be looking at these more on a case-by-case basis. This also means that we have to be at the top of our game, because it makes no sense to encrypt something that someone else can easily read. So, it's only working when it's really providing the security we think it provides."

Gerhard Gohr

Business unit lead of IT planning and control at the Information und Technik North Rhine-Westphalia (IT.NRW), Germany.

This is also becoming critical for businesses operating in complex regulatory environments, such as financial services. In Europe, the regulators in certain verticals have been warning about cloud concentration risk: i.e., that you should not have too many "eggs in one cloud provider's basket."[51] A senior executive of a large US-based bank adds, *"Hybrid sovereign models are the most practical way forward. This hybrid journey will start with small steps and then – depending on the success of the projects with respect to security, etc. – it would be taken forward."*

Hybrid cloud makes it possible for organizations to balance the needs of innovation and sovereignty. They help organizations to comply with data-sovereignty requirements while preserving the control and flexibility they need to use data as part of their overall business strategy.

69%

of organizations said they believe that data encryption is a means to manage the "non-sovereignty" aspects of cloud today.

Consider end-to-end encryption and key management solutions:

In our research, 69% of organizations said they believe that data encryption is a means to manage the "non-sovereignty" aspects of cloud today. Gerhard Gohr, business unit lead of digital lab and service development at the Information und Technik North Rhine-Westphalia (IT.NRW), Germany – central statistical and IT services provider of North Rhine-Westphalia, says, *"The encryption of data can be a potential alternative to sovereignty in special cases. Of course, this requires more calculation power and sometimes takes away usability, but it's an option, or it's even mandatory when we are really sharing or transporting data from A to B. But that's only one of the solutions we have to look into, while we will be looking at these more on a case-by-case basis. This also means that we have to be at the top of our game, because it makes no sense to encrypt something that someone else can easily read. So, it's only working when it's really providing the security we think it provides."*

Today, to manage non-sovereignty issues, organizations focus on end-to-end data encryption when data is in transit and ensuring they hold the **"keys"** to data when it is stored at rest in the cloud. Options of fully self-owned and managed keys as well as client managed keys using cloud provider solutions exist today. Organizations will see a trade-off in ease of support and simplicity of use compared to using the vendor's standard "key management" offerings, but this will give them control over accessibility of their data. For instance, Deutsche Bank has stated that the firm will hold the keys to decrypt data as they migrate key applications to the cloud.[52] With "keep-your-own-keys" solutions, the data owner can define user-access permissions and enforce consistent policies across the hybrid multi-cloud environment. Thales and Google Cloud collaborated in 2020 to offer new capabilities where encryption keys are owned and controlled by the security teams while helping to fulfill heightened regulatory requirements amid today's widely distributed workforce.[53]

Beyond encryption and gatekeepers, implementing other prerequisites for operating in a "zero-trust environment" – including active protection such as adequate access controls, auditing, logging, automated checks/alerts on correct use of encryption/key management, etc., becomes important to enable better visibility and create boundaries between users and data and applications.

Prepare for a multi-cloud architecture:

"Multi-cloud" refers to the use of two or more cloud providers for cloud services. Wells Fargo, for instance, has multi-cloud as part of its cloud strategy. *"When we think of workload, we typically think about applications but, for us, I think the value will be in the ability to move our data from one to the other without leaving that data behind,"* says Mike Telang, Wells Fargo's executive vice-president and head of enterprise architecture.[54]

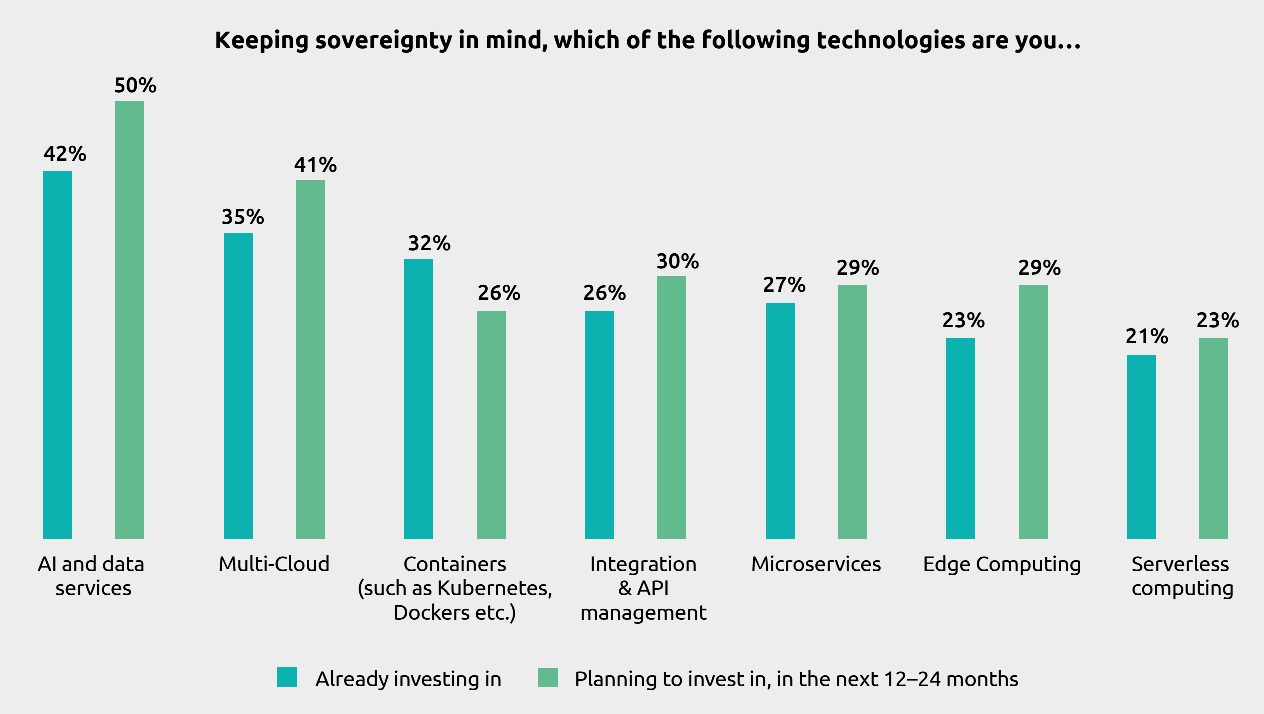
Factoring in a multi-cloud roadmap and architecture model is critical to ensuring that data and application integration and controls for the organization are in place. Holger Lehmann, head of management staff and Public Relations Officer of the German Federal Center for Information Technology, sums it up, *"There are two aspects of sovereign cloud for us: technology and data. On the technology side, there must be options and no vendor lock-in. You need a multi-vendor strategy that ensures portability and can react to market changes. Cloud market is an oligopoly, and this makes it difficult to act confidently. On the data side, you need to have control over what happens to data. For us, it is crucial that European/German standards be adhered to. The more insensitive the data, the more likely a public cloud can represent a solution under certain standards. However, sensitive data must remain in sovereign cloud."*

However, preparing for multi-cloud architecture also requires organizations to understand the different complexities that it brings – from architecture, interoperability, security to networking, compliance, and cost. Multi-cloud architecture also takes longer to design and build. Organizations need to develop potential solutions for these challenges up front in their planning:

- **Architecture and design:** The architecture and design process becomes more complex to create, implement, maintain, and adapt. While at application level, it may be possible to define a common architecture that can span multiple clouds, at infrastructure level, particularly for security and networking, there are differences that must be understood in order to protect and optimize the solution, dependent upon the cloud platforms used.
- **Portability:** Designing for portability at the different levels of the architecture requires intent and investment and a pragmatic approach to the trade-off between portability benefits and the cost of re-engineering a solution to move platforms. Design principles such as modularity, loose coupling, microservice architectures, etc., can help reduce the impact of porting workloads and, with the correct architectural approach, including containerization and serverless designs, portability between public clouds at workload or composite-service level can be achievable. Our research shows that organizations are investigating various technologies while keeping sovereignty in mind (see Figure 19):

Fig.19

AI and data services, microservices and containerization are the top technologies that sovereignty-conscious organizations are currently investing in



Source: Capgemini Research Institute, Cloud Sovereignty Survey, May–June 2021, N = 1,000 organizations.

- **Integration:** Organizations need to ask themselves, if the data and applications are spread across multiple clouds, how can seamless interoperability be facilitated across different cloud environments? In particular, it is critical for organizations to understand how best to achieve integration in a multi-cloud environment while considering sovereignty and regulatory compliance. This must be considered for scenarios, such as distributed data platforms and application platforms across different cloud environments and geographies.
- **Security:** How can control be established to monitor security and regulatory compliance, especially if the multi-cloud environment is operated by both local and non-local vendors?
- Also, as workloads are distributed across multiple environments, how can transparency and openness be established? What are the monitoring tools that can support the different APIs and platforms?

Engage and educate stakeholders:

Organizations also need to educate their stakeholders regarding the different aspects of sovereignty in order to ensure the same level of understanding of the topic across the organization. CIOs need to define "cloud sovereignty" for their organizations and align stakeholders to follow this definition across all levels.

50%

plan to invest in AI and data services and 41% plan to invest in multi cloud in the next 12-24 months, keeping sovereignty in mind.

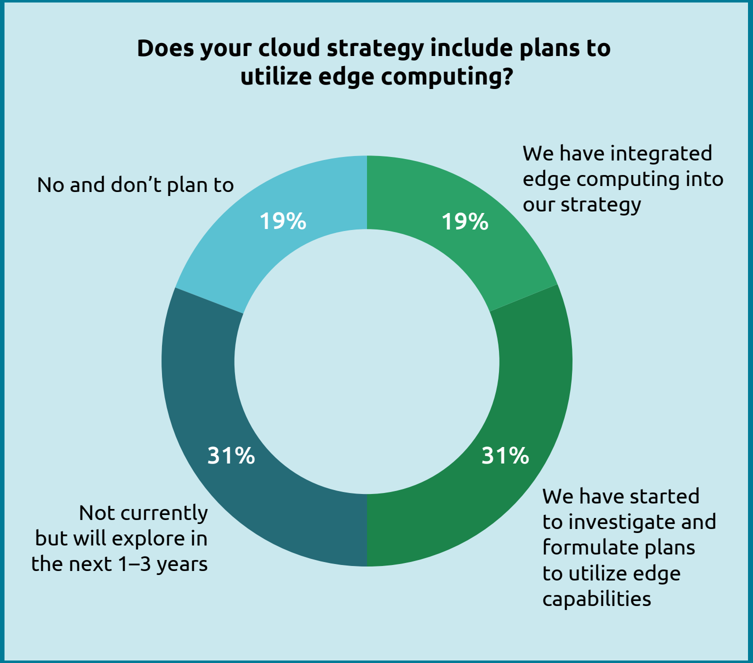
Edge computing for sovereignty and compliance

Edge-computing solutions are considered one of the driving forces behind the fourth industrial revolution. According to estimates,[55] edge computing has become a top priority for C-suite executives and is critical to meeting strategic business objectives. The report predicts that, by 2023, over 50% of the new enterprise IT infrastructure deployed will be at the edge, rather than in corporate data centers, up from less than 10% in 2020. By 2024, the number of apps at the edge will have increased by 800%. Our research also shows that half of the organizations consider edge a part of their overall cloud strategy.

Edge computing provides extra control of the location of data compared to that provided by the public cloud.

Fig.20

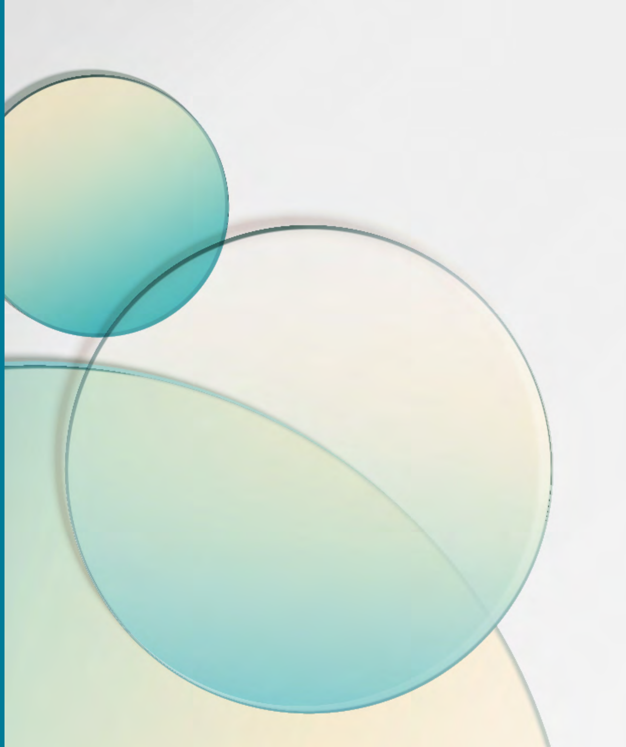
50% of organizations currently look at edge as a part of their overall cloud strategies; 31% plan to explore in the next three years



Source: Capgemini Research Institute, Cloud Sovereignty Survey, May–June 2021, N = 1,000 organizations.

Businesses can keep data in the local jurisdictions where their end users are located through an edge architecture that places workloads at the edge of the network and not in the public cloud data center, which may be subject to different laws. This is especially useful when different states introduce their own data regulations.

Edge computing and sovereignty go hand in hand, as edge makes it easier to know where data resides and who governs it. As Figure 19 highlights, nearly 30% of organizations in our research plan to invest in edge – simply to ensure sovereignty. One of the major drivers of the "move to edge" is compliance with sovereignty imperatives or sectoral regulations. A senior technology executive from Sydney Trains Australia says,*"Sovereignty is, by default, a part of edge computing. I suppose if it's edge, then it is sitting locally anyways, it is not going anywhere. Obviously, it comes down to your infrastructure, how you design your infrastructure. We would connect those edge devices to our approved infrastructure, but the compute would be happening on the edge; in our case, by default, that is happening here in Australia."*



DEVELOP the potential of sovereign cloud

Apart from regulatory compliance, sovereign cloud should also be viewed from the lens of "trust" and wider business benefits. To realize its full potential, organizations need to:

Assess the value proposition of sovereign cloud (e.g., trust, security, collaboration)

Our research shows that 63% of organizations rate trust and a secure cloud environment for data as the biggest benefit offered by sovereign cloud.

For instance, France will confer the "trusted cloud" label on providers complying with their sovereignty principles and conditions set by the National Cybersecurity Agency of France (ANSSI).[56] A trusted cloud will invariably help organizations to develop a reliable cloud infrastructure for hosting applications.

At the same time, sovereign cloud offers opportunities for collaboration, especially in regulated and critical sectors such as life sciences and the public sector (as indicated above).

Explore synergies through ecosystem participation:

Organizations can consider being part of broader sovereignty-related ecosystems that bring in different sector stakeholders, technology providers, and government representatives. Possible synergies include:

- **Driving benefits from ecosystems:** This can help firms to access and share data in trusted data spaces. For instance, GAIA-X proposes a reference architecture, based upon open-source license and common standards, for interoperability of data among participants.[57] IT.NRW's Gerhard Gohr points to the benefits of sharing resources,*"With a sovereign cloud setup, the biggest benefit for the public sector is that we can share resources. We can then really get benefits from scalability because we are not providing a certain service to 10 or 100 people. We provide a certain service to millions of people and then scalability enables digital transformation on a much broader scale. So, there are a lot of services we could provide that we are not able to provide currently on our own."*

- **Developing new solutions:** Within the "trusted cloud" environment, sovereign cloud can help in developing new solutions, especially in data-sensitive sectors like the public sector and healthcare. The French government, for instance, is planning to digitize public-sector initiatives with citizens and institutions with its sovereign cloud infrastructures. Sarah Wilkinson, CEO of the UK's NHS Digital, has outlined the benefits from standardization of cloud infrastructure, saying,*""Greater standardization of data, infrastructure, platforms, and APIs will create a health and care system that is more joined-up, safer, and efficient. Connected systems ensure that clinicians have access to all relevant and appropriate patient data from all care providers and settings and ensure that data is communicated between systems with absolute fidelity."*[58]

Evaluate permissive "open-source" solutions:

Organizations can also opt for technologies and tools that help them to access, deploy, and move data and applications, and serve as a gateway to the sovereign cloud. These include:

- Open-source solutions for containers and orchestration (e.g., Kubernetes) to drive, deploy, and scale containerized applications. Open-source applications and open standards also help to bring in more choices and control, such as API interoperability. Our research shows that 32% of organizations are investing in container-related applications today, and that 26% plan to invest within the next two years.
- Storage and processing.
- Federated single-sign access and controls (e.g., OpenIAM).

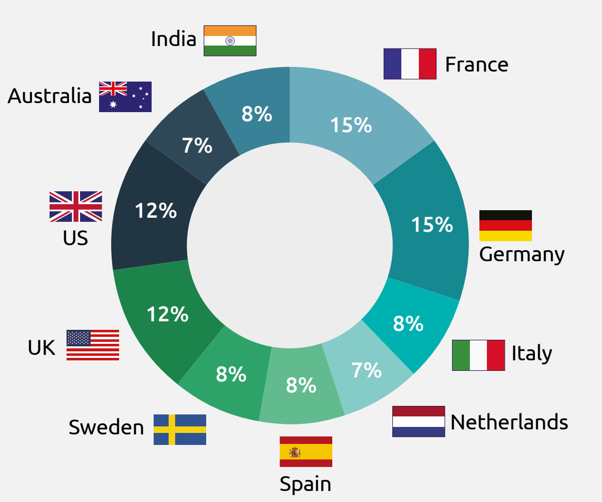
Conclusion

The growing focus on data protection and the increasing need for a trustworthy data infrastructure will drive sovereignty to a central role in the cloud market. Initiatives such as GAIA-X, as well as emerging complexity in regulatory landscape further enhance the push for cloud sovereignty from countries and regulators. While firms believe that cloud sovereignty is gaining importance, it is time that they view this topic beyond the regulatory lens. In addition, they need to consider the wider potential benefits, such as collaborative data ecosystems and a trusted infrastructure to move critical applications. To achieve that goal, the first step for organizations is having an "enterprise view" of their data – where it is stored, how well it is categorized in terms of their criticality to the nation and organization. Organizations then need to assess their internal readiness to embed sovereign cloud, making key components – including localization, interoperability, portability, customer controls, openness, and transparency part of their cloud environment – which will enhance readiness to implement sector relevant use cases. Firms that proactively incorporate these components into their cloud infrastructure will not only manage regulatory risk but will also build trust and a competitive advantage in the digital age.

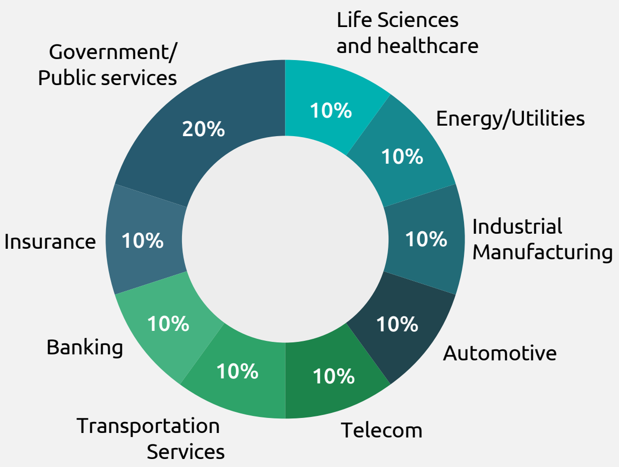
Research Methodology

We surveyed executives from 1,000 organizations at the level of director or above between May and June of 2021. All of these organizations (excluding public sector) reported revenues of more than USD1 billion for the last financial year. In addition, we conducted 14 in-depth interviews with technology and business executives.

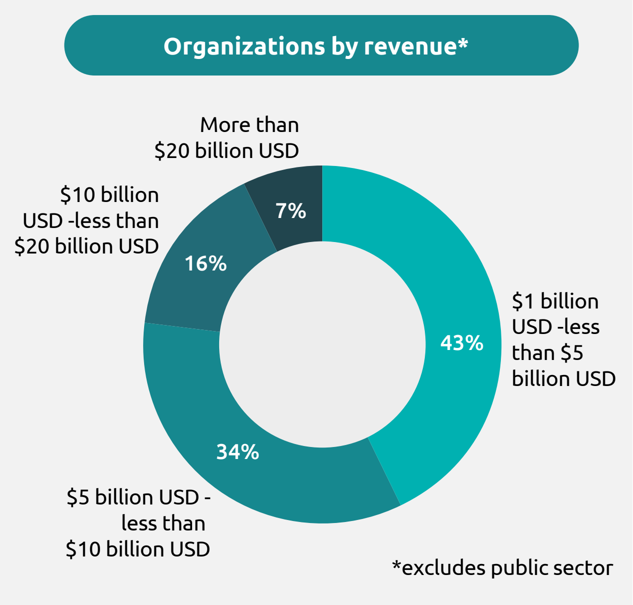
Organizations by country



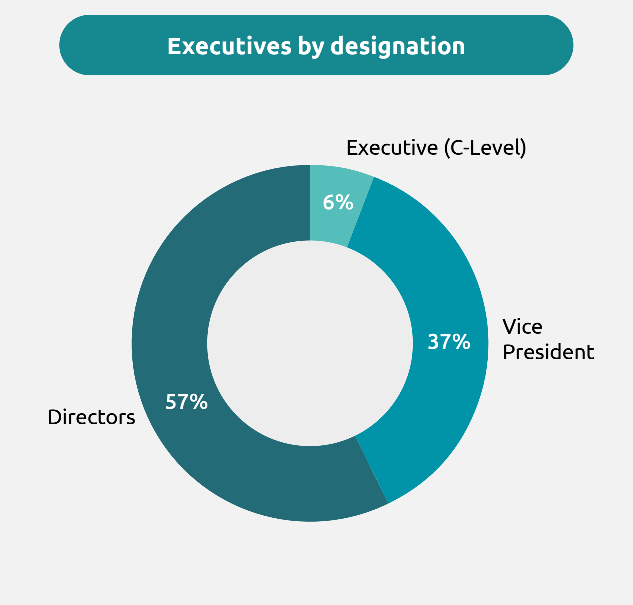
Organizations by sector

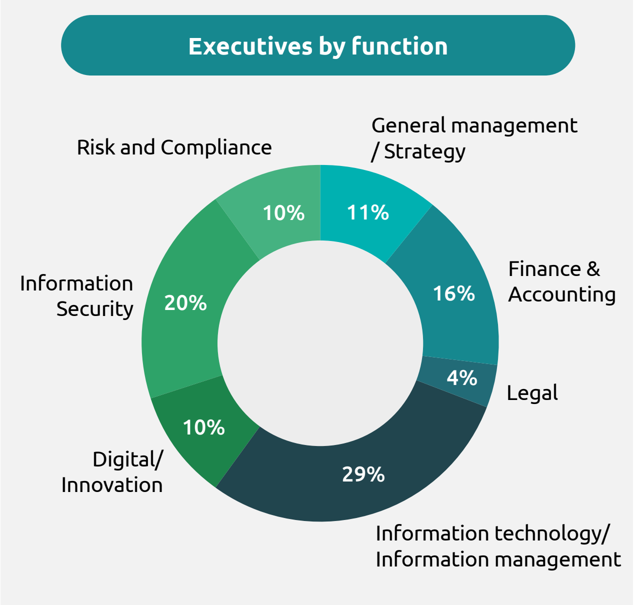


Source: Capgemini Research Institute, Cloud Sovereignty Survey, May–June 2021, N = 1,000 organizations.



*excludes public sector





Source: Capgemini Research Institute, Cloud Sovereignty Survey, May–June 2021, N = 1,000 organizations.

Reference

1. IDC, “IDC forecasts worldwide "Whole Cloud" spending to reach $1.3 trillion by 2025,” September 2021.
2. Diginomica, “Capital One closes its data centres and goes all in with AWS,” January 2021.
3. Justice.Gov, “Dag, Cloud Act.”
4. European Commission, “Standard Contractual Clauses (SCC) - Standard contractual clauses for data transfers between EU and non-EU countries,” accessed 4th July 2022.
5. Digital strategy. EC. Europa.EU, “Towards a next generation cloud for Europe,” October 2020.
6. EUR-Lex, “The European Data Strategy,” February 2020.
7. EUR-lex. Europa.EU, “A European strategy for data.” February 2020.
8. Digital strategy. EC. Europa.EU, “Cloud computing.”
9. Digital strategy. EC. Europa.EU, “Towards next generation cloud Europe,” October 2020.
10. EUR-lex.Europa.EU, “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – 2030 Digital compass: the European way for the digital decade,” March 2021.
11. European Commission, “Data Act: Proposal for a regulation on harmonised rules on fair access to and use of data,” February 2022.
12. Lemonde Informatique.Fr, “The government shifts its strategy to the trusted cloud,” May 2021.
13. OO Drive, “Cloud de Confiance new label for state cloud doctrine,” June 2021.
14. IT-Planungsrat, “IT Planning Council – Cloud computing and digital sovereignty, 29th meeting, Decision 2019/38,” June 27, 2019; Open Government Partnership, “Data Sovereignty in North Rhine-Westphalia.”
15. Trusted-cloud. De, “About trusted cloud.”
16. Discussion with Harald Joos, CIO bei Bundesministerium der Finanzen held on September 15, 2021
17. Discussion with Harald Joos, CIO bei Bundesministerium der Finanzen held on September 15 2021; Heise Online, “Sovereign cloud: Microsoft lures the federal government with a free test platform,” April 2021.
18. Telekom, “T-Systems and Google Cloud Partner to Deliver Sovereign Cloud for Germany” Aug 9, 2021
19. DTA.gov.au, “Whole-of-government Hosting Strategy.”
20. Government News, “Data hosting rules could be tightened,” July 2020.
21. T News.AU, “News, NSW government signs on with Vault Cloud,” July 2020.
22. Telecoms, “Calao presents Italy’s plan for cloud autonomy,” September 2021.
23. Pilsbury Law, “China adopts new data security law,” July 2021.
24. Lexology, “Detailed draft implementing regulations released for China’s Personal Information Protection Law and Data Security Law,” November 2021.
25. Carnegie India, “How would data localization benefit India?” April 2021.
26. Atlantic Council, “Waving the flag of digital sovereignty,” December 2019.
27. CIO, “With hyperforce, Salesforce is enabling public cloud,” December 2020.
28. Datacenter News, “NTT’s data center projects buzzing in Hong Kong, India and the UK,” September 2020.
29. Datacenter dynamics, “NTT plans $2 billion data center investment in India, aims to double data capacity,” March 2021

30. Cloud. Google, “Engaging in a European dialogue on customer controls and open cloud solutions,” September 2020.
31. Microsoft, “Answering Europe’s Call: Storing and Processing EU Data in the EU,” May 2021.
32. Forbes, “Azure Arc – Extending Microsoft cloud services to data centers and mainstream cloud platforms,” September 2020.
33. CRN, “Google Cloud Anthos: Hybrid AI and 5 other new features,” August 2020.
34. Cloud. Google, Anthos.
35. AWS, “Amazon EKS Anywhere,” accessed 6th July 2022.
36. Microsoft, “Azure Stack Hub: Bringing the agility and innovation of cloud computing to your on-premises environment,” accessed 6th July 2022.
37. Capgemini, “Capgemini and Orange announce that Bleu will start engaging with customers by the end of 2022,” June 2022.
38. Thales Group, “Thales introduces S3NS in partnership with Google Cloud and unveils its offering in a first step towards the French Trusted Cloud Label,” June 2022.
39. Azure. Microsoft, “New Azure region coming to China in 2022,” March 2021.
40. Capgemini Research Institute, “Data sharing masters: How smart organizations use data ecosystems to gain an unbeatable competitive edge,” July 2021.
41. HPE, “How swarm learning provides data insights while protecting data sovereignty,” June 2021.
42. World Today News, “Docaposte, AstraZeneca and Impact Healthcare create a platform for hosting and processing health data,” June 2021.
43. Federal Ministry of Economic Affairs and Energy, bmwi.de, “Dr. Michael Bolle, Managing Director, Robert Bosch GmbH about GAIA-X,” June 2020.
44. The Banker, “European banks form public cloud club,” February 2021.
45. Gartner, “Will GAIA-X impact I&O strategies in Europe during 2021?” March 2021.
46. NHS Digital, “NHS and social care data: off-shoring and the use of public cloud services,” accessed July 27, 2021.
47. HHS, “Guidelines on HIPAA and cloud computing,” November 2020.
48. VentureBeat, “France says Google, Microsoft cloud services are OK for sensitive data,” May 2021.
49. DataCenter Knowledge, “Bank of England warns on risks of banking’s reliance on cloud computing,” July 2021.
50. Enisa.Europa.EU, “Securing Cloud services for health,” January 2021.
51. Tech Monitor, “Microsoft heralds a new ‘decentralised’ era for the cloud,” March 2021.
52. DataCenter Knowledge, “Deutsche Bank to move ‘heart’ of IT systems into Google’s cloud,” December 2020.
53. Thales Group, “Thales and Google Cloud join forces to deliver breakthrough capability for enterprises to control their data in the cloud”, July 2020.
54. AI Trends, “Multi-cloud strategy a fit for large enterprises; Wells Fargo finding it helps to have flexibility to move data,” September 2019.
55. IDG Connect, “Edge Computing Solutions Powering the Fourth Industrial Revolution”, January 2021.
56. Venture Beat, “France says Google, Microsoft cloud services are ok for sensitive data,” May 2021.
57. GAIA-X.EU, “What is GAIA-X, Data spaces.”
58. IT Proportal, Features, “Why IT in the public sector is moving to the sovereign cloud,” September 2019.

Authors

Marc Reinhardt
Executive Vice President and Head of Public Sector, Capgemini
marc.reinhardt@capgemini.com

Thierry Daumas
EVP, Head of Projects & Consulting, CIS
thierry.daumas@capgemini.com

Papa Ibrahima Ndao
Vice President, Cloud & Enterprise Architecture
papa-ibrahima.ndao@capgemini.com

Subrahmanyam KVJ
Senior Director, Capgemini Research Institute
subrahmanyam.kvj@capgemini.com

Ron Tolido
EVP, CTO, Insights and Data Global
ron.tolido@capgemini.com

Vincent Charpiot
Executive Vice President - Cloud Infrastructure & Cybersecurity Managing Director, Americas at Capgemini
vincent.charpiot@capgemini.com

Angélique Lallouet
Executive Vice President, France, Services & Public Sector BU Head
angelique.lallouet@capgemini.com

Nancy Manchanda
Program Manager, Capgemini Research Institute
nancy.manchanda@capgemini.com

Anne-Laure Thieullent
Managing Director, Artificial Intelligence & Analytics Group Offer Leader
annelaure.thieullent@capgemini.com

Dapo Adekola
Vice President, Chief Technology & Innovation Officer (CTIO) - Cloud
dapo.adekola@capgemini.com

Jerome Buvat
Global Head of Capgemini Research Institute
jerome.buvat@capgemini.com

The authors would like to thank Franck Greverie, Fernando Alvarez, Stefan Zosel, Stuart Ball, Niels Lemmens, Manas Deb, Jean Marc Defaut, Jean Philippe Defrance, Leo Isaac-Dognin, Nicolas Gaudilliere, Guy-Michel Pambi, Sergio Henrique Werner, Kai Schroeder, Dolo Miah, Jose Kuzhivelil, Gunnar Menzel, Pierre-Adrien Hanania, Jitendra Thethi, Raghu Vempati, Michael Hansen, Thomas Heimann, Geert Van der Linden, Martin Lambinet, Rens Huizenga, Sam Price, James Dunn, Gurpreet Sachdeva, Naveen Kumar S, John Ogden, Yannick Martel, Brian Hammond, Donna Urraca, Sandeep Sachdeva, Marcel Van der Burg, Philippe Roques, Ryan Murphy, Giulia Carsaniga, Eymeric Tabou, Shamik Mishra, Sabine Bogner, Christian Janssen, Carlos Ferrero Calle, Rob Kernanhan, Maria Fritzsche, Luis Delabarre, Annabelle Ducellier, Oliver Jones, Ulrich Bonfig, Vijayalakshmi K, Praveenkumar Sharma, Mohinder Sawhney, Abirami B, Soumik Das and Rupali Chakraborty for their contribution to this report.

About the Capgemini Research Institute

The Capgemini Research Institute is Capgemini's in-house think tank on all things digital. The Institute publishes research on the impact of digital technologies on large traditional businesses. The team draws on the worldwide network of Capgemini experts and works closely with academic and technology partners. The Institute has dedicated research centers in India, Singapore, the United Kingdom, and the United States. It was recently ranked number one in the world for the quality of its research by independent analysts.
Visit us at www.capgemini.com/researchinstitute/

For more information, please contact:

Contact

Global
Marc Reinhardt
Executive Vice President and Head of Public Sector, Capgemini
marc.reinhardt@capgemini.com

Germany
Frank Jacobsen
Head of Public Sector
frank.jacobsen@capgemini.com

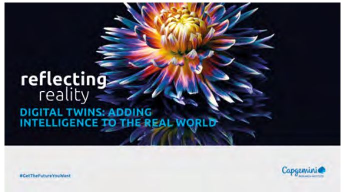
Netherlands
Pieter Nieuweboer
Cloud COE Leader
pieter.nieuweboer@capgemini.com

France
Sergio Werner
Head of Cloud COE - South & Central Europe
sergio-henrique.werner@capgemini.com

UK
James Dunn
CIS Cloud Portfolio Leader
james.dunn@capgemini.com

Spain
Gabriel Enriquez
Head of Cloud COE - Spain
gabriel.enriquez-molina@capgemini.com

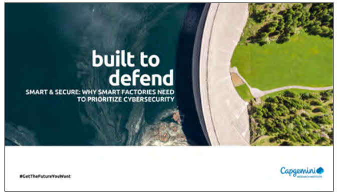
Discover more about our research



Digital Twins: Adding Intelligence to the real world

Capgemini
Conversations for tomorrow
Intelligent Industry: The Next Era of Transformation
#GetTheFutureYouWant

Conversations for Tomorrow #3: Intelligent Industry


built to defend
SMART & SECURE: WHY SMART FACTORIES NEED TO PRIORITIZE CYBERSECURITY
#GetTheFutureYouWant
Capgemini

Why smart factories need to prioritize cybersecurity

Sustainable operations

Capgemini
The data-powered enterprise
Why organizations must strengthen their data mastery

The data-powered enterprise: Why organizations must strengthen their data mastery

Capgemini
Accelerating the 5G Industrial Revolution
State of 5G and edge in industrial operations

Accelerating the 5G Industrial Revolution State of 5G and edge in industrial operations

Capgemini
NEXT DESTINATION: SOFTWARE
How automotive OEMs can harness the potential of software-driven transformation

Next Destination: Software How automotive OEMs can harness the potential of software-driven transformation

Data mastery: How data-powered organizations outperform their competitors

Capgemini
DATA SHARING MASTERS
How smart organizations use data ecosystems to gain an unbeatable competitive edge

Data sharing masters: How smart organizations use data ecosystems to gain unbeatable competitive edge

+Subscribe to latest research from Capgemini Research Institute

Receive copies of our reports by scanning the QR code or visiting https://www.capgemini.com/capgemini-research-institute-subscription/

Capgemini Research Institute

Fields marked with an * are required

First Name *

Last Name *

Email *

□ By submitting this form, I understand that my data will be processed by Capgemini as indicated above and described in the Terms of use . *

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of over 340,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2021 global revenues of €18 billion.

Get the Future You Want | **www.capgemini.com**