MAKING IT REAL

4 steps to cloud sovereignty in the public sector

1. Executive summary

From GAIA-X to geopolitics, external factors have amplified public sector interest in sovereign clouds. This report will guide you through the what, why and how of these transformative solutions.

Public sector organizations are grappling with many fast-moving challenges, not least growing citizen demands for evidence-based decision-making and seamless, scalable services.

To address these challenges, organizations need to respond and adapt faster than ever before. By combining data from different institutions, and applying analytics, AI and automation, they will be able to identify and deliver up-to-the-minute solutions and offer a better user experience.

Adopting the cloud makes it simpler, cheaper and faster to do this. But to keep the trust of citizens, public sector organizations must also guarantee the privacy and security of their data, along with continuity of critical services. And many have concerns – sometimes misconceptions – about the ability of cloud technologies to provide such assurances.

76% of public sector respondents globally believe their organization will adopt cloud sovereignty to ensure compliance with regulations and standards.
- Capgemini Research Institute: The Journey to Cloud Sovereignty

Interest in cloud sovereignty is growing in the sector

In recent years, growing regulation, geopolitical unrest and initiatives like GAIA-X have also increased the desire of governments to have more control over their digital destiny.

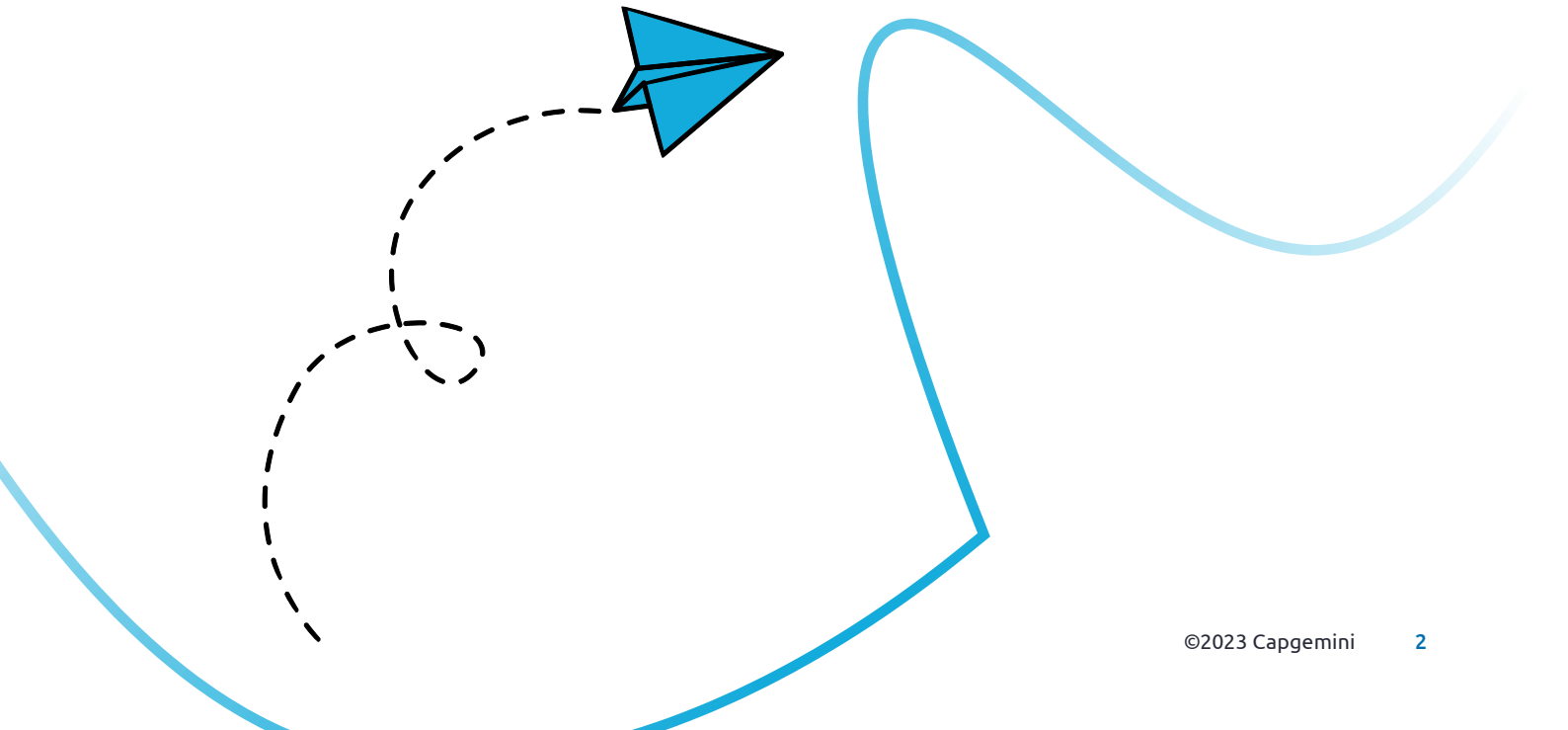
A sovereign cloud gives them an appropriate level of control over their data, technology and operations in a dedicated environment. In doing so, it provides compliant, secure access to the efficiency, agility, scalability and rapid innovation of the cloud.

Encouragingly, as demand for sovereign clouds has grown, so has the number of off-the-shelf options available. Buyers can now choose from solutions that meet different levels of sovereignty, both from global hyperscalers and emerging regional players.

Public sector organizations that take advantage of this growing choice will be able to confront and tame the monster under the bed: the complex, ever-changing regulation around data. They will also be able to protect that data from extra-territorial access and build resilience against crises. And, by sharing data safely, they will ultimately be able to offer the seamless public services citizens expect – affordably and sustainably.

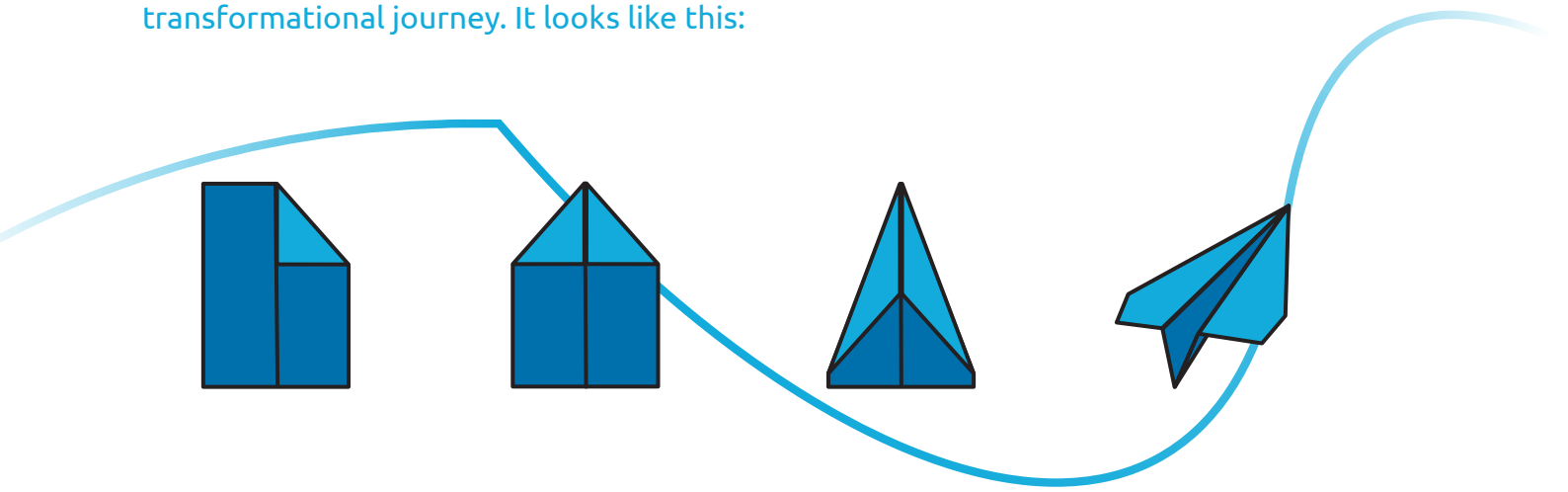
Over time, we believe that this sovereign thinking will also extend to encompass broader aspects of a digital economy, such as the supply chains for raw materials and components.

57% of public sector respondents globally said initiatives that prioritize sovereign cloud will become stronger, compared with 47% of organizations globally.
- Capgemini Research Institute: The Journey to Cloud Sovereignty



How can you make cloud sovereignty real in your organization?

At Capgemini, we use a four-step process to guide public sector organizations along this transformational journey. It looks like this:



Plan Sovereign Cloud → Implement Sovereign Cloud Transformation → Operate Sovereign Cloud → Explore Innovation Potential

Step 1: Plan
(Advisory): Get clarity – define your needs, classify your data and meet your regulatory requirements

Step 2: Implement
(Cloud Transformation): Choose a technology platform based on the outputs of step 1. Then build a sovereign landing zone and develop the cloud-native apps that will deliver your service or workload

Step 3: Operate
(Sovereign Cloud Operations): optimize your solution for performance, cost-efficiency, compliance and resilience over time – including upskilling your teams to manage a multi-cloud environment

Step 4: Explore
Tap into the full transformational power of the cloud in and beyond your state, region or country

Cloud sovereignty opens the door to transformation in the public sector, but the topic can be complex to navigate. This report will debunk the myths and demystify the process.

In an environment that is becoming more challenging and less certain, can you afford not to make cloud sovereignty real?

Chapter 1

AN INTRODUCTION TO CLOUD SOVEREIGNTY

What is a sovereign cloud, why does it matter and how has it become such a hot topic for public sector organizations? We answer some common questions.

How did we get here?

Over the last decade or more, organizations around the world have rapidly adopted public cloud services from global hyperscalers. However, European governments operate in a jurisdiction without its own native hyperscale cloud providers. Many perceive a particular need to protect their sensitive data, and have questioned how their values and interests can be protected within an international digital system that relies significantly on companies based elsewhere.

The EU initiative GAIA-X is a product of this wider context. Founded in 2019, its aim is to establish a trusted environment in which data can be shared and used. Cloud sovereignty is a prerequisite for its success, because data needs to be secured and protected in order to be shared. So, cloud sovereignty (which includes data sovereignty) enables GAIA-X to exist. This helps to explain why the concept of cloud sovereignty – previously only discussed in limited circles – is now more widely understood.

But GAIA-X isn't the only factor driving the need for cloud sovereignty. Before the COVID-19 pandemic, important geopolitical shifts were taking place and a more multipolar world was emerging. The pandemic then accelerated digitization across the sector, along with the expectations of citizens for data-driven government. And, for the same reason as GAIA-X, sovereignty is the key to delivering this improved user experience.

The invasion of Ukraine has compounded the case for sovereignty still further by showing the need for autonomy over technology as well as energy and raw materials. As Roberto Viola (Director General, Transparency at the EC's Directorate-General for Communications Networks, Contents and Technology) observed at the European Business Summit 2022: "War has brought a reality check that the digital giant we are trying to create has feet of clay."

So, in today's uncertain world, cloud sovereignty is not only the foundation of modern public services. It is also a strategic imperative for preventing your data, technology or operations from becoming geopolitical bargaining chips. And in our view, demand for it is here to stay.

65% of the world's population will have its personal data covered under modern privacy regulations by 2023.
- Gartner, March 2022

What is a sovereign cloud?

There are many definitions in circulation. This is the one we use at Capgemini: A sovereign cloud is a cloud computing environment that is owned, governed and managed within a single nation, region or jurisdiction and complies with its laws.

That means that the data within the environment stays in your chosen location and is stored, processed and shared in line with the regulation for that jurisdiction. It also means you have full control and transparency over your environment - from who can access your data (and with whom you exchange it) to how often you switch providers or scale up a service. Essentially, a sovereign cloud solution can give you more control over your digital destiny.

68% of public sector respondents globally expect a sovereign cloud to provide a trusted and safe cloud environment for data.
- Capgemini Research Institute: The Journey to Cloud Sovereignty

Why does it matter?

By storing your data in a dedicated environment, you can keep it private and protected from access by foreign powers.

-- §For public sector organizations, particularly in Europe, this is central to maintaining the trust of citizens. But data sovereignty is only one aspect of cloud sovereignty.
At Capgemini, we look at the issue through three lenses:

- **Data sovereignty.**
  As we've explained, this ensures you comply with data regulation while giving you control over your data and allowing you to share it safely.
- **Technical sovereignty.**
  This gives you transparency and control over the technology your service is running on (for example, through open source), as well as the freedom to change providers and run interoperable applications.
- **Operational sovereignty.**
  This provides assurance that your data complies with national cybersecurity standards and wider regulations over time. It also gives you the flexibility to restore your service quickly following a crisis.

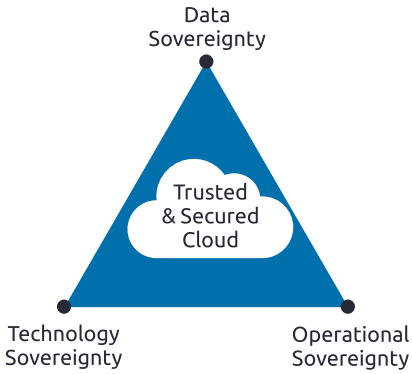


Figure 1: How Capgemini views cloud sovereignty

Each service or workload will require a different level of sovereignty across each of the three areas. It will also involve making trade-offs between innovation and risk management. We will explain this in more detail in Chapter 2.

How does cloud sovereignty open the door to transformation?

With some notable exceptions, including in the UK, Estonia and Belgium, relatively few public sector organizations have so far moved their services or workloads to the cloud.

Often, a fear of "getting it wrong" – particularly regarding regulation around data – is behind this hesitancy. Spending taxpayers' money on technical, hard-to-grasp solutions can seem too big a risk to take, especially without the financial incentives for change that exist in industry.

At Capgemini, though, we do not view regulation as a blocker to adopting the cloud. Instead, we see data as the new infrastructure for innovation, and regulation as a way of releasing its full potential by making sure it flows safely.

In that sense, regulation such as the EU's General Data Protection Regulation (GDPR) operates like a traffic light. It may annoy people when it's red, but it exists to make sure we can cross an intersection safely and reliably – even in heavy traffic.

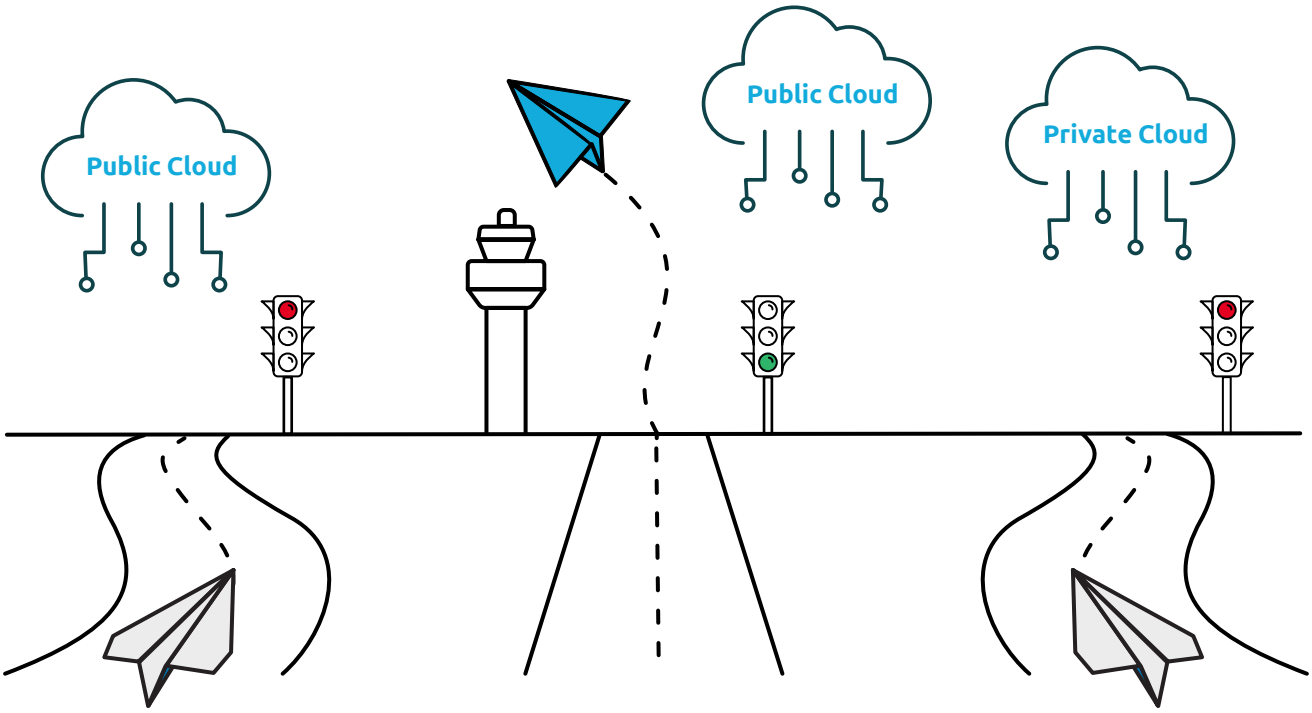


Figure 2: Regulation does not block innovation; it gives it the green light

By moving to a sovereign cloud, you are creating a safe, trusted environment – whether that's in a public or a private cloud.

So, sovereignty is not an end in itself, but an enabler for realizing the benefits of the cloud. These include not only seamless, scalable new models for delivering public services, but also the ability for public sector organizations to access and use each other's data.

How does sovereignty enable this transformation?

- By opening up data spaces and ecosystems that allow you to share data between agencies or silos while preserving privacy. So you can use AI technologies to implement a "once-only" or "tell us once" principle.
- By giving you the choice of avoiding vendor lock-in, so you can join up your digital services end to end.

61% of public sector respondents globally believe a sovereign cloud will allow them to share data with trusted partners in their ecosystem.
- Capgemini Research Institute: The Journey to Cloud Sovereignty

Let's get technical

Confusion can easily arise when you are dealing with a complex technical topic. Here are three questions we commonly encounter.

1. **Should a sovereign cloud always be a private cloud?**

   No. Private clouds are very expensive and slow to develop, as you need to build and manage the infrastructure yourself. You also do not benefit from the scale and innovation of the hyperscalers.

   What's more, national, regional or global cloud providers can now meet the privacy and regulatory requirements of most workloads or services. (That is unless you need an extremely high level of sovereignty, in which case your service may need to run on on-premises software.)

   An ideal solution is a multi-cloud approach, in which an organization uses two or more different cloud providers to meet different needs and spread risk. A sovereign cloud is only one aspect of this broader strategy.

How do sovereign clouds relate to data spaces, data ecosystems or GAIA-X?

A data space is a relationship between trusted partners who follow the same standards around storing and sharing data openly. A data ecosystem is a platform where trusted partners share data and use it to create value.

The EU initiative GAIA-X combines both aspects. It is a federated data infrastructure which unites cloud service providers and users in an open and transparent data-sharing environment that is subject to EU laws. (See page 5: How did we get here?)

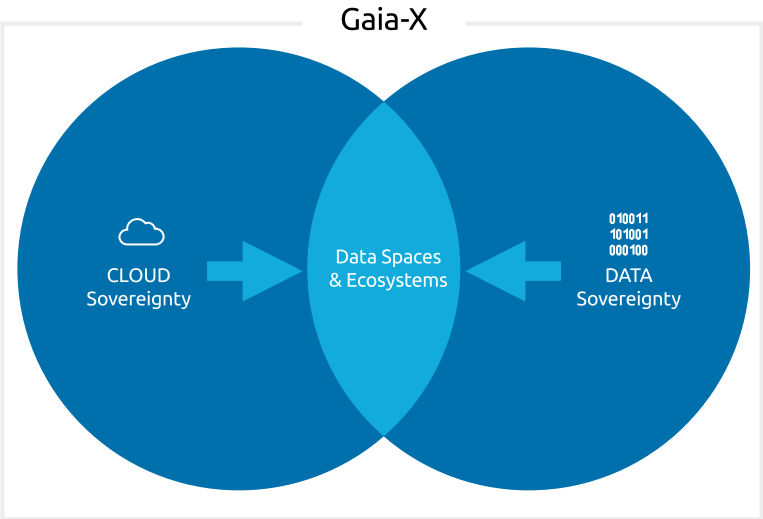


Figure 3: How sovereignty enables new data spaces and ecosystems

2. **What's the difference between cloud sovereignty and digital sovereignty?**

   Cloud sovereignty is having control over the platforms, infrastructure and software (including data) that enable your processes in the cloud. As such, it is one part of the much broader concept of digital sovereignty, which encompasses aspects far beyond the cloud – from the tangible, such as components like microchips, to the intangible, such as laws and ethics.

   While these wider areas are not within the scope of this report, they are relevant to highly secure agencies like defense. For example, it is important to have trust, transparency and autonomy over the systems that control how you protect your country and your allies – including deterrents.

   In future, though, it is likely that more public sector organizations will need to expand the scope of their sovereignty to include these non-cloud aspects. Recent history has shown how interruptions to supply chains can cause prices to soar (energy) and production to stop (microchips). Efforts to build sovereignty over these broader aspects will also build resilience.

   The big takeaway? Sovereignty is not going anywhere; in fact, it will only become more important.

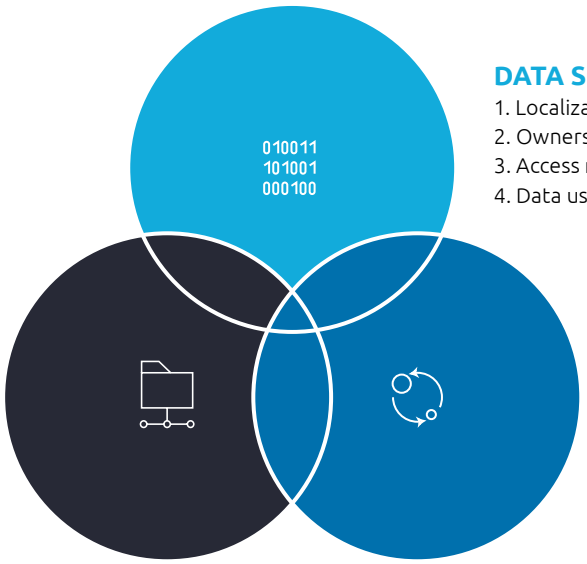
Chapter 2

MORE TO SOVEREIGNTY THAN THE MONSTER UNDER THE BED

The three dimensions of cloud sovereignty and what they offer public sector organizations

Compliance with regulation around data privacy, access and control (the monster under the bed) is currently the main driver for public sector organizations adopting a sovereign cloud. But interest in technical and operational sovereignty is starting to grow too.

In this chapter, we will provide more detail on the three dimensions of the sovereignty triangle. This includes what each could look like in practice (which will vary depending on your use case and level of sovereignty needed), and how you might benefit. Note that technical constraints mean that no one solution can offer both full innovation and the highest level of security.



DATA SOVEREIGNTY
1. Localization/residency
2. Ownership/privacy
3. Access management
4. Data usage transparency

TECHNICAL SOVEREIGNTY
5. Reversibility and portability
6. Technology transparency and interoperability
7. Regional ecosystem of partners

OPERATIONAL SOVEREIGNTY
8. Operational resilience
9. Regulatory compliance
10. Technical and organizational measures

Figure 4: The 10 key requirements for sovereignty in the cloud

	Data sovereignty	Technical sovereignty	Operational sovereignty
What it covers	• Self-determination/control • Compliance with data regulation around: » localization/residency » access management » data transparency	• Reversibility and portability • Technology transparency and interoperability • A regional ecosystem of partners	• Operational resilience • Monitoring regulatory compliance over time • Meeting cybersecurity standards and guidelines
Possible outcomes, depending on your use case and level of sovereignty	• Data complies with local data laws by staying within your specified area (state, country or region), accessed and controlled only by people in that area • All your data is encrypted and either you, or a trusted provider/operator within your specified area, own the key • You stay in full control of your data, from storing, processing and deleting it to moving it between agencies or authorities • Your cloud provider regularly validates compliance – for example, by proving that only authorized users have accessed your data	• Choose your technology (open source where possible, to give you more control) • Avoid becoming locked-in with a provider by building technology-agnostic services • Have visibility of the technology and product roadmaps underpinning your cloud environment, and build technical knowhow internally • Benefit from "build once, run everywhere" software that allows you to switch services between providers • Pick and choose your level of sovereignty according to each workload or service • Trust that everyone in your ecosystem of partners abides by the same sovereignty standards and access rights	• Control Identity and Access Management (IAM) for your operation teams, so only authorized users can access your environment – and you can audit it yourselves • Use open-source software and application platform interfaces (APIs) to give you full control and transparency, especially over your most sensitive workloads • Restore your service quickly in the event of a crisis • Develop a process or make a trusted partner responsible for monitoring compliance over time • Your vendor or provider has the necessary national and international security certifications • Makes sure you comply with regulation and cybersecurity standards over time, and are either in control, or can take control, of your cloud environment
Why it matters	Enables you to meet your regulatory requirements, while giving you tight control over critical or sensitive data in general and allowing you to share it safely	Gives you transparency over your technology, as well as the ability to shift workloads between multiple cloud platforms and change providers easily	Makes sure you comply with regulation and cybersecurity standards over time, and are either in control, or can take control, of your cloud environment
How it has helped public sector organisations	Client: A research institution, Germany Solution: IONOS During the pandemic, a number of state governments wanted to use a research institution's education platform for home-schooling. But it was on-premises and in pilot mode. Capgemini re-built the solution and moved it on to a national superscaler to mitigate client concerns about hosting student data on a public cloud. We then scaled it by a factor of 20 in just a few months.	Client: A UK public security authority Solution: AWS As it deepened and broadened its use of the cloud, this public security authority wanted to increase its level of control and therefore sovereignty. AWS evolved its existing solution to meet the authority's new requirements (including full encryption) on its platform for managing public security and law enforcement.	Client: A French public administrator Solution: OVH This French public body wanted to host its employee data and run internal processes on the cloud, while keeping that data private. We moved it to a national superscaler, which assures the data remains in France.

Moving to the cloud: three common myths debunked

1. Data

"If I move my data to a US hyperscaler, the US government will be able to access it through the CLOUD Act."

68% of public sector respondents globally cited potential exposure to extra-territorial laws or access by foreign governments as a concern with the cloud environment.
- Capgemini Research Institute: The Journey to Cloud Sovereignty

Adopted in 2018, the CLOUD Act is designed to help the US government identify and fight serious crime including terrorism and child exploitation.

A common misconception is that the Act enables US law enforcement agencies to access any personal data stored outside of the country by US-headquartered cloud providers. In fact, the Act only applies to communications data. According to the US Department of Justice, such data could include "the contents of communications, subscriber information, and data stored remotely on behalf of a user ('in the cloud')." Accessing finance data is expressly forbidden by the Act and carries a penalty.

In other words, the perceived risks to data privacy are very different from the reality of what the Act can do. This is borne out by the actual instances of the Act being enforced: according to Amazon, there were zero enforcements on EU data in 2021.

Nonetheless, under the CLOUD Act, it is theoretically possible for the US government to access data held by a US-based hyperscaler – even if this runs counter to regulation such as GDPR.

Efforts are underway to tackle this mismatch. At the end of 2022, the Biden government and the European Commission submitted a proposal to harmonize data privacy within the EU-US Data Privacy Framework. But the activist Max Schrems believes the proposal is not in line with the GDPR and will be rejected by the Court of Justice of the EU (CJEU) after a third legal review. We expect concrete results at the end of Q1/Q2 2023.

Until then, the two regulatory systems remain fundamentally incompatible, creating legitimate concerns for public sector organizations that need to take care of citizen data. One way to manage that risk is for national governments with what the Act calls "robust protections for privacy and civil liberties" to draw up their own, CLOUD-Act-based bilateral agreement with the US. The UK-US Data Access Agreement is one such initiative.

Moving sensitive or personal data to a sovereign cloud is another option. In these environments, all data is encrypted, and the supplier – even if it is a US-based hyperscaler – cannot access the key to unencrypt it. It is up to the owner of the sovereign cloud to decide whether to hand over the key.

Explore more:
You can access the CLOUD Act on the website of the United States Congress: https://www.congress.gov/bill/115th-congress/senate-bill/2383/text

Alternatively, the US Department of Justice has published a helpful paper that explains the Act in simple terms and includes a set of user-friendly FAQs: www.justice.gov/opa/press-release/file/1153446/download

2. Technology

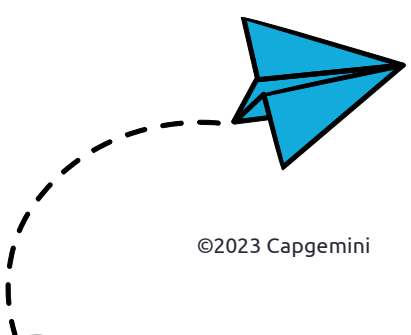
"If I move to the cloud, I will become locked-in to a particular provider like I am on-premises."

66% of public sector respondents globally cited a lack of interoperability between applications as a concern with the cloud environment.
- Capgemini Research Institute: The Journey to Cloud Sovereignty

Vendor lock-in, where the cost of switching to a different product or service becomes so high that the buyer is forced to stay where they are, is a common issue in legacy environments. However, it can also happen in the public cloud. And the more tailored the technology, the bigger the risk.

Take data. To create the most value from yours, you need to be able to move it freely, to take advantage of new technologies as they emerge. Yet you can only do so if your application programming interface (API) allows you to "port" data to another provider. OpenAPIs, built on open source, allow you to move as much data as possible. But if your provider has custom-built your API, and the software around it, you are "locked" in and can only look longingly at the shiny new products and services on other platforms. The vendor can put their prices up, or lower the quality of their service, and you still cannot get away.

That said, vendor lock-in in the cloud is by no means inevitable and can be avoided by careful planning and diversifying to reduce your risk. We work with clients to build an architecture that makes it possible to port and deploy applications across cloud platforms. It is part of the reason we recommend implementing a multi-cloud strategy, which allows you to allocate workloads between two or more public clouds according to cost or other criteria.



3. Operations

"If my service goes down in the cloud, I won't be able to get it back up again."

74% of public sector respondents globally cited the security and resilience of the provider as a concern with the cloud environment.
- Capgemini Research Institute: The Journey to Cloud Sovereignty

It would be unacceptable for any technology failure to interrupt or compromise the delivery of a critical public service. Yet the more services you move to cloud environments, the more dependencies you create.

To build resilience into your sovereign cloud strategy, you need to do two things:

1. Balance the risks against the gains. If a service is not business-critical, or you have a contingency plan to cover outages, the innovative features you gain from a public cloud could outweigh the risks. But if you need to run a service constantly, or at least be able to recover it easily, you need to assure this by design and avoid dependencies at all costs.

2. Diversify your supplier base. If you rely too heavily on one provider (particularly one that uses specific proprietary functions), it will be difficult to switch to another platform in the event of an outage or other crisis. Spread the risk and you can get back up and running much faster. Alternatively, if you use open-source software, in the worst-case scenario you can rebuild your service with another supplier or in your own private cloud. That is why the demand for open-source software goes up in line with the need for sovereignty.

Chapter 3

STARTING THE JOURNEY TO SOVEREIGNTY

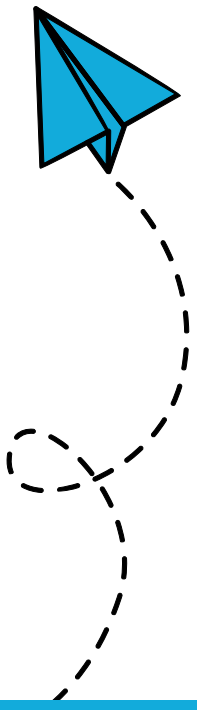
4 steps to realizing the transformative power of the cloud

There are real, executable solutions on the market now for moving to the cloud with confidence and trust. But navigating the number of providers and deployment models available can be a challenge, particularly when the picture is constantly moving. The terminology providers use can also be misleading; a "trusted" cloud is not necessarily sovereign, for example.

Our vendor-agnostic process will help you to feel confident you are choosing the right sovereign cloud platform (and trusted provider) for your needs in the long term.

In this chapter, we will guide you through how we do it. As we have said before, though, no technology is perfect for all situations, and technical restrictions mean there will always be trade-offs.

34% of public sector respondents globally that are already focusing on cloud sovereignty (or plan to do so in the next year) need more clarity on the subject.
- Capgemini Research Institute: The Journey to Cloud Sovereignty



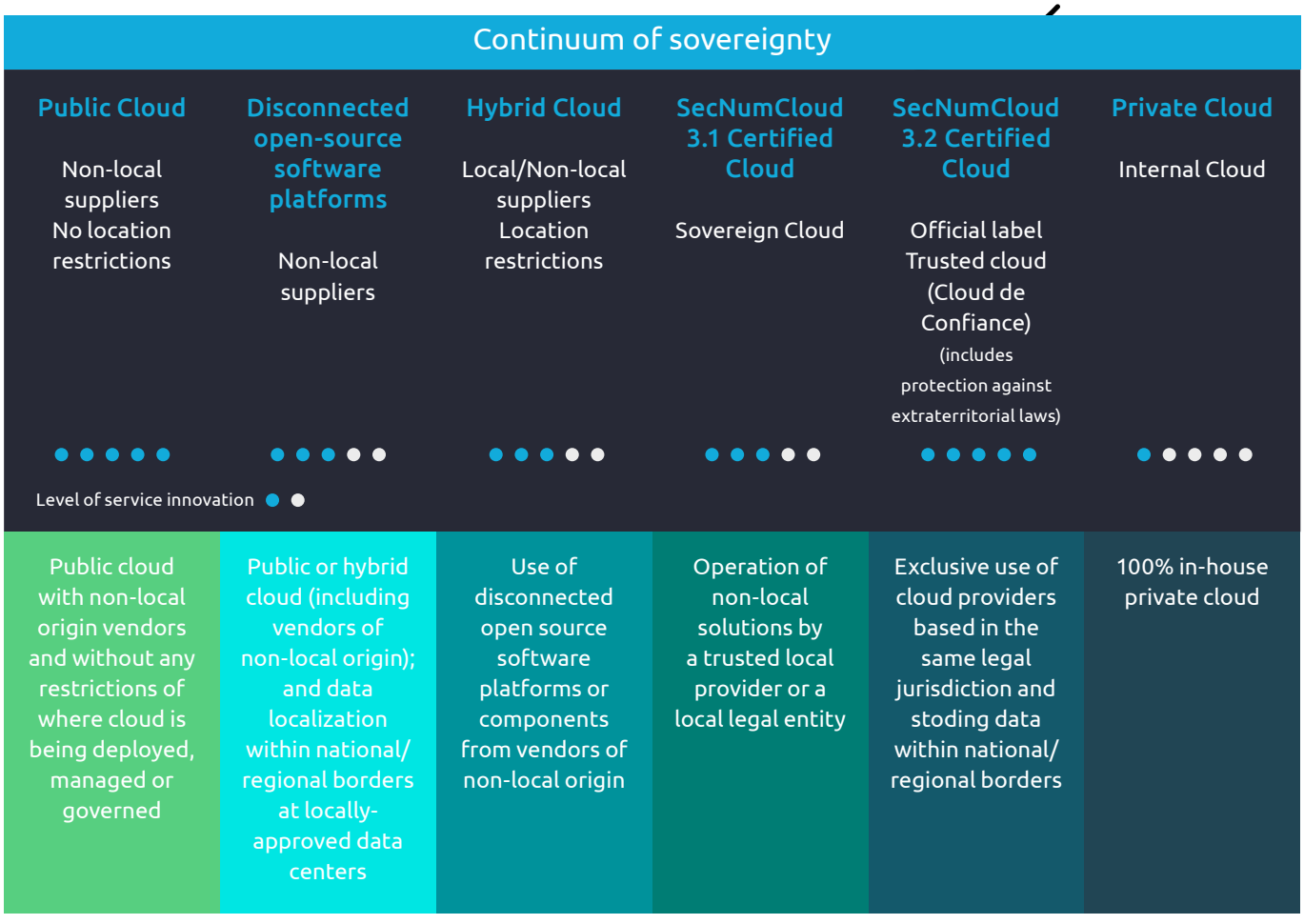
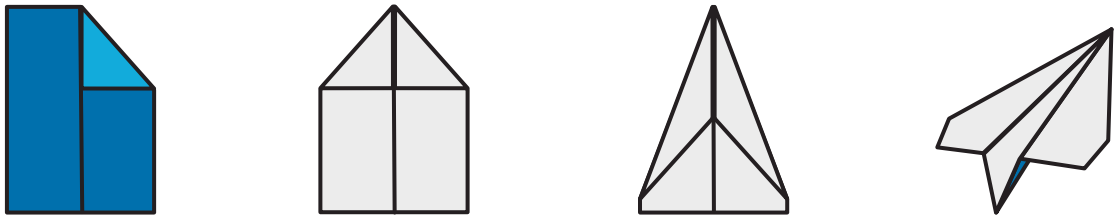


Figure 5: The continuum of sovereignty

Plan, implement, operate, explore



Plan Sovereign Cloud | Implement Sovereign Cloud Transformation | Operate Sovereign Cloud | Explore Innovation Potential

Step 1: Plan
(Advisory services): Get clarity – define your needs, classify your data and meet your regulatory requirements

Step 2: Implement
(Cloud Transformation): Choose a technology platform based on the outputs of step 1. Then build a sovereign landing zone and develop the cloud-native apps that will deliver your service or workload

Step 3: Operate
(Sovereign Cloud Operations): optimize your solution for performance, cost-efficiency, compliance and resilience over time – including upskilling your teams to manage a multi-cloud environment

Step 4: Explore
Tap into the full transformational power of the cloud in and beyond your state, region or country

STEP 1: Plan

The aim of this stage is to break down your big ideas and uncertainties into smaller, more manageable questions about your goals and needs across the three dimensions of sovereignty. The answers we uncover together will lay vital groundwork for the rest of the process.

First, though, you need to establish the right questions to ask. Through our Sovereign Innovation Hub (a kind of workshop), we can map out a cloud strategy based on your starting point – whether that's your business model or your need for data security.

Next, we establish what sovereignty means to you and what you want it to achieve. Is your main aim to keep tighter control of your data? Or do you want to be able to recover services within days by switching providers in a multi-cloud environment? Do you need to understand what's under the bonnet of your technology? Or is it more important to consume something innovative as a service – no questions asked? And how many dependencies can you accept?

Whatever your aim, as a public sector organization, you will need to look at the monster under the bed and ask: What data regulations apply to our data at home and overseas? Once you understand that, you can classify your data accordingly to those requirements. (See Making it real: classifying your data.)

Outcome: a framework or decision tree for identifying the best technology to build your sovereign landing zone – including the technical and organizational measures that will ensure compliance. Plus a database of all your data, tagged according to the level of privacy it requires.

Example: A financial regulator we worked with wanted to move services to a public cloud. But as the client held personal as well as financial data, classifying that data properly was a crucial element of the execution plan. We also created a decision tree to help choose the right technical and organizational solution for different demands, including compliance with regulation. The blueprints we refined during the project could help other financial institutions regulated by the same authority.

Making it real: classifying your data

You need to classify your data in order to choose a sovereign cloud platform that meets your privacy

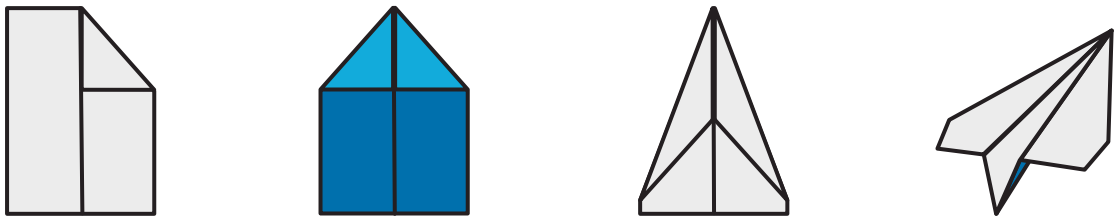
demands. Yet there is currently no public standard for the categories to use.

At Capgemini, we have created a simple system to use as a starting point for discussions with clients. We have based it on the essence of the rules in Europe and beyond; you may need to add more levels to reflect the regulation in your jurisdiction.

- **Level 1 (public):** any non-personal, unregulated data.
- **Level 2 (personal):** the GDPR defines this as "any piece of information that relates to an identifiable person", such as an email address. This data can only be accessed by people who need to work with it for a defined purpose.
- **Level 3 (sensitive):** data that is classified by law as private or "official secrets", such as health data or confidential company data (in Germany, the relevant law is §203 StGB). Only people the law views as trained to handle that data can do so.
- **Level 4 (classified):** information which the law (in Germany, the VS-NfD) defines as classified. Only people with the relevant security clearance can handle this data and it cannot be shared outside of the agency.

Once you have classified your data as levels 1-4, you can also classify the various components of your sovereign cloud infrastructure. We can then make sure the levels correspond.

67% of public sector organizations globally are either working on a classification system for their data and assets in the cloud or plan to do so in the next 12-24 months.
- Capgemini Research Institute: The Journey to Cloud Sovereignty



Plan Sovereign Cloud | **Implement Sovereign Cloud Transformation** | Operate Sovereign Cloud | Explore Innovation Potential

Step 1: Plan
(Advisory): Get clarity – define your needs, classify your data and meet your regulatory requirements

Step 2: Implement
(Cloud Transformation): Choose a technology platform based on the outputs of step 1. Then build a sovereign landing zone and develop the cloud-native apps that will deliver your service or workload

Step 3: Operate
(Sovereign Cloud Operations): optimize your solution for performance, cost-efficiency, compliance and resilience over time – including upskilling your teams to manage a multi-cloud environment

Step 4: Explore
Tap into the full transformational power of the cloud in and beyond your state, region or country

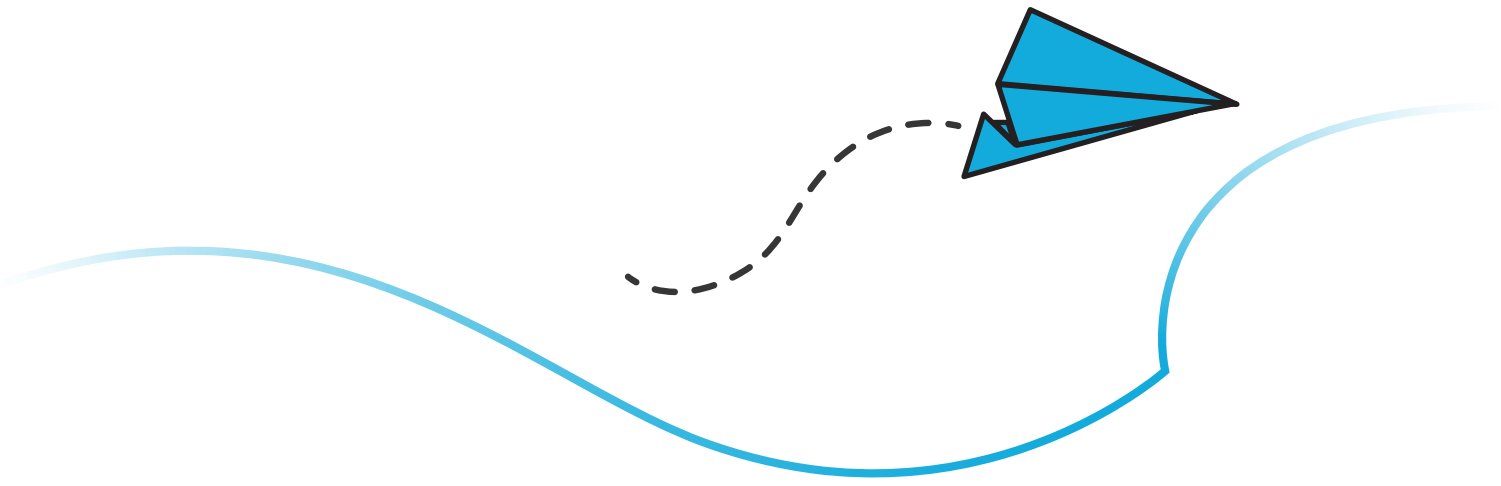
Step 2: Implement

Here, we take the measures, data classification and framework from step 1 and work with your technical teams to implement a solution that meets your needs.

We start by assessing cloud platform providers through the lens of your requirements in each area of sovereignty. This includes answering questions such as:

- Data: does the provider give you visibility of, and control over, its administrative access to your data?
- Technical: does the solution share any intuitive interoperability and migration features with other cloud solutions you use?
- Operational: does the provider have control over the technology powering the cloud?

We then use the chosen technology to build your sovereign landing zone in the cloud, incorporating end-to-end encryption and services for managing who accesses your environment and how.



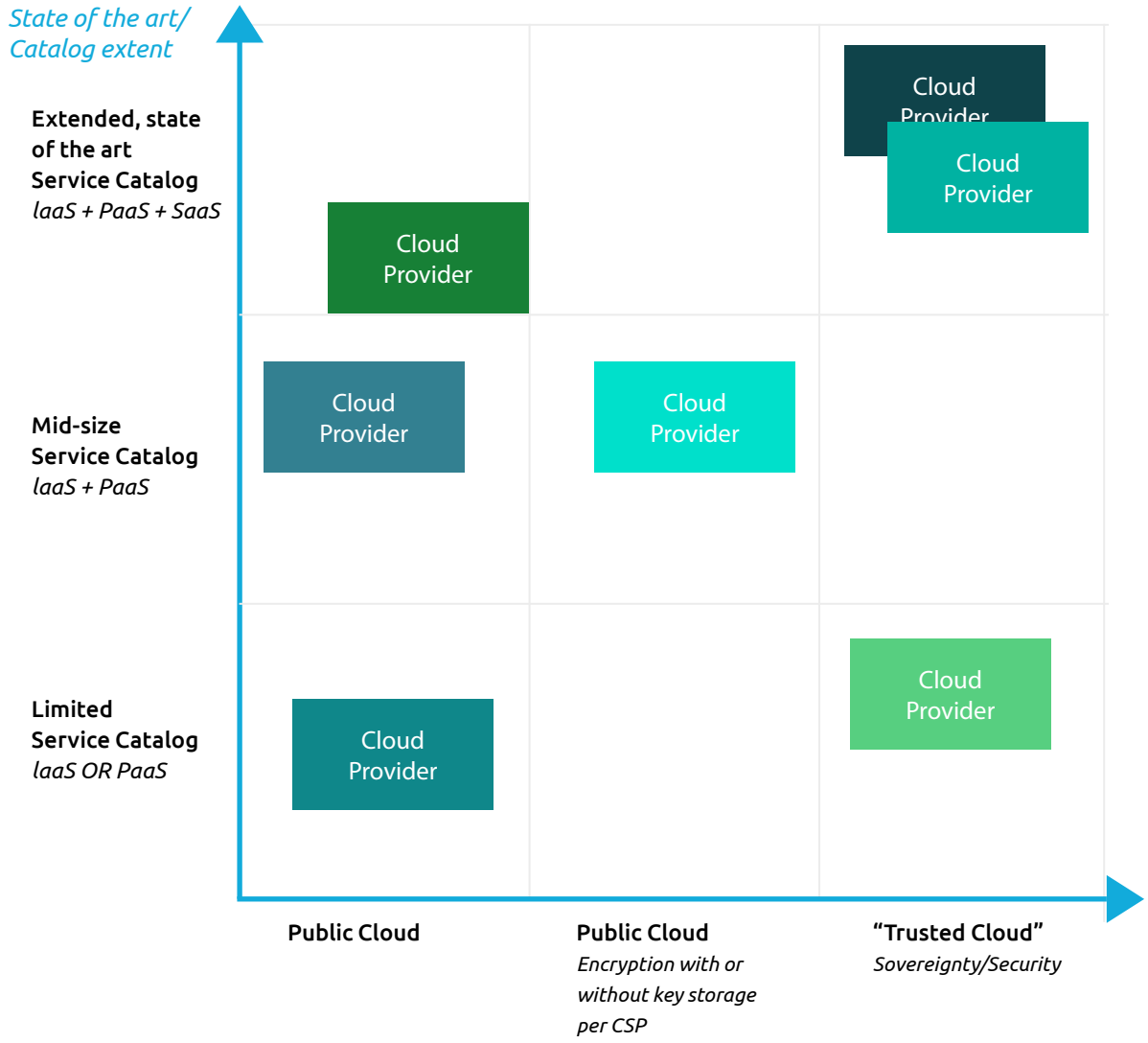


Figure 6: One way of mapping different solutions against your regulatory and business needs

Encryption is key to cloud sovereignty because it decouples your data and software from your provider's cloud infrastructure, creating a compliant environment. You can then control who can access that environment through identity and access management (IAM) and key management.

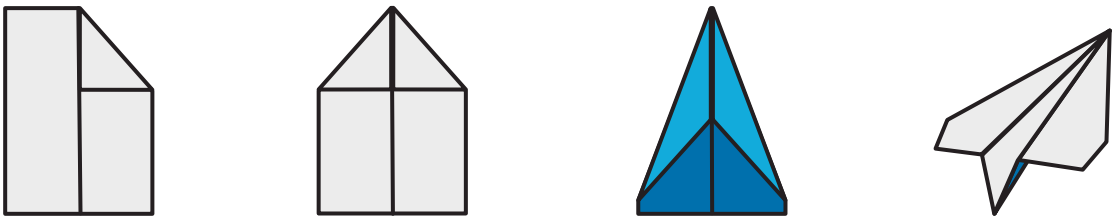
Finally, we develop intelligent, cloud-native apps within your landing zone to deliver your service or workload.

85% of public sector organizations globally consider identity and access management, along with data encryption, when choosing a cloud platform provider.
- Capgemini Research Institute: The Journey to Cloud Sovereignty

Outcome: an efficient, cost-effective and scalable service or workload that offers a good user experience and runs on a sovereign landing zone that ticks all your regulatory boxes.

Example: A public security authority decided to move its immigration and passports service to a public cloud to meet growing business demands for flexibility, speed and cost savings.

But it needed a secured and safe environment to process the personal data of millions of citizens.
By encrypting the authority's data, Capgemini helped to transform the service, saving around $30m through advanced cloud technologies, automation and AI. The carbon footprint of the service's IT systems also decreased significantly.



Plan Sovereign Cloud → Implement Sovereign Cloud Transformation → **Operate Sovereign Cloud** → Explore Innovation Potential

Step 1: Plan (Advisory): Get clarity – define your needs, classify your data and meet your regulatory requirements

Step 2: Implement (Cloud Transformation): Choose a technology platform based on the outputs of step 1. Then build a sovereign landing zone and develop the cloud-native apps that will deliver your service or workload

Step 3: Operate (Sovereign Cloud Operations): optimize your solution for performance, cost-efficiency, compliance and resilience over time – including upskilling your teams to manage a multi-cloud environment

Step 4: Explore Tap into the full transformational power of the cloud in and beyond your state, region or country

Step 3: Operate

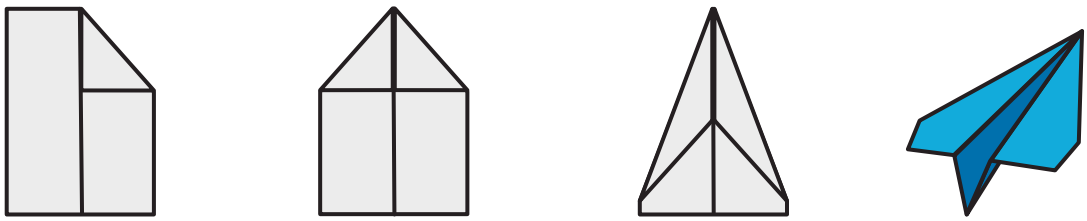
It is one thing to build the perfect sovereign cloud environment for your service or workload. It is another to make sure it is sustainable over the long term.

Operate is therefore an ongoing process of managing your cloud-based applications so they are as flexible, resilient and cost-effective as possible. It can include establishing which operational tasks need to stay within the sovereign environment and which can be outsourced to a trusted partner. It also involves making sure your people have the technical skills needed to manage a multi-cloud environment.

Keeping up with fast-moving regulation around data and security is another important element. As long as you are compliant and have built flexibility into your solution, you can swap services between providers and mix cloud with on-premises solutions to achieve the best results for you, your users and the taxpayer.

Outcome: A secure, compliant and cost-effective solution for the lifetime of the contract.

Example: The French cyber security agency, ANSSI, has created two certifications (SecNumCloud 3.1 and 3.2) for solutions that achieve a certain level of sovereignty and meet local regulations. To qualify, providers must abide by the principles of operational sovereignty we set out on chapter 2, as well as with principles around data and technical sovereignty. Today, a handful of public cloud providers based in France are providing SecNumCloud-certified solutions as a way of modernizing public services.



Plan Sovereign Cloud → Implement Sovereign Cloud Transformation → Operate Sovereign Cloud → **Explore Innovation Potential**

Step 1: Plan (Advisory): Get clarity – define your needs, classify your data and meet your regulatory requirements

Step 2: Implement (Cloud Transformation): Choose a technology platform based on the outputs of step 1. Then build a sovereign landing zone and develop the cloud-native apps that will deliver your service or workload

Step 3: Operate (Sovereign Cloud Operations): optimize your solution for performance, cost-efficiency, compliance and resilience over time – including upskilling your teams to manage a multi-cloud environment

Step 4: Explore Tap into the full transformational power of the cloud in and beyond your state, region or country

Step 4: Explore

So, you now have a sovereign cloud platform – part of your multi-cloud approach – that enables you to combine data from different silos safely to give citizens a seamless, scalable experience. How could it help you take public services to the next level – Government-as-a-Service or Platform?

Holding another session of the Sovereign Innovation Hub could help you think about the longer-term opportunities for your organization. You could also look to your peers for inspiration.

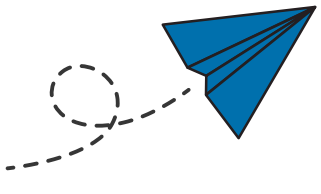
Below, we have suggested three ideas to explore.

1. **Save time and effort for citizens.**
   The once-only principle states that citizens and businesses should not have to provide data to government that is already in its hands. So, a change of address reported to one service would automatically update across all agencies.

   When combined with AI technologies, this principle could see a citizen go online to claim maternity benefits, and subsequently receive alerts from the education agency to register their child for a place at nursery. It is about identifying events that will affect the user and proactively providing e-services, rather than putting the onus on the citizen to ask for them.

2. **Share apps as well as data.**
   In chapter two, we shared the example of a German research institution that scaled up its online education platform during the pandemic so several states could use it. But there is no reason why we could not develop apps in one country and share the code base with others – saving money and allowing more people to benefit from a good idea. Models devised along the lines of GAIA-X would enable this kind of cross-pollination.

3. **Become a lean, clean, cost-effective machine.** In a cloud environment, some services can be completely automated while others can help you achieve more with fewer people. (Public sector organizations can struggle to recruit talent, particularly for tech jobs.) A highly efficient, automated service in the cloud also contributes to the sustainability goals of your organization.



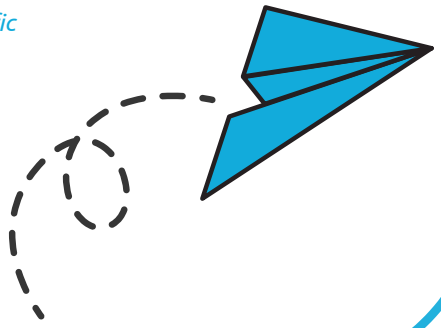
Examples: Leading governments are adopting Government-as-a-Platform approaches. Estonia's X-Road platform links the information systems of all its departments, enabling the "once-only principle" we described above. Germany's Portalverbund aims to link all the portals from federal, state and local authorities into a single network, so citizens and businesses can access any of around 600 digitized government services. And the UK's Government Digital Service has created building blocks – such a common payment solution – that all departments can use to build services. What's more, Capgemini's 2022 eGovernment Benchmark found that European governments pre-fill over two-thirds of online application forms with information previously provided to them.

As cloud sovereignty matures, public sector organizations expect its benefits to grow.

Percentage of respondents who expect to see "high benefits" from deploying sovereign cloud in specific public sector contexts.

- *62% Connecting data infrastructure across smart city services.*
- *61% Sharing data across departments (data-driven government).*
- *61% Supporting citizens digitally 24/7 through chatbots.*

- Capgemini Research Institute: The Journey to Cloud Sovereignty



What should you take away from all this?

It is important for public sector organizations to consider cloud sovereignty, but discussions around this complicated topic are often overheated.

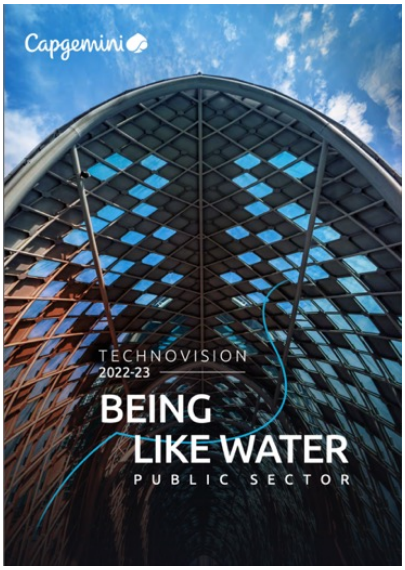
Fortunately, there are solutions and best practices available to simplify and cool it down. And if you implement a concrete plan, as we have described here, you will be able to move a huge set of workloads on to modern public cloud infrastructures.

The key is to develop expertise in your own teams, build trust in cloud technology and create an ecosystem for sharing and using data that complies with regulation. In doing so, you will open the door to fast, modern and innovative public services.

Explore more

You can read about our approach to cloud transformation projects at: www.capgemini.com/insights/expert-perspectives/cloud-transformation-the-keys-to-success.

For the latest public sector trends, download our annual publication, TechnoVision, at: https://www.capgemini.com/insights/research-library/technovision-202223-public-sector-edition/



AUTHOR:

Stefan Zosel

Capgemini Government Cloud Transformation Leader

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 organisation of 360,000 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, fuelled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2022 global revenues of €22 billion.

Get the Future You Want | www.capgemini.com

GET THE FUTURE YOU WANT

MACS_2023