



Digital sovereignty with purpose:

Balancing innovation,
resilience, and compliance



Table of contents

01	Dealing with the fast-shifting boundaries of digital sovereignty	4
02	Making the right choice for your organisation	10
03	Five steps to digital sovereignty	17
	Conclusion: Future-ready sovereignty	25
	Market spotlights	26
	Authors	48



A combination of evolving digital ecosystems, tech dependencies, regulatory pressures, and geopolitical tensions have brought digital sovereignty to the top of the strategic agenda.

This is also an agenda that's becoming increasingly complex and multidimensional as the focus of digital sovereignty stretches beyond data residency to encompass operational independence, human dependencies, and survivability. And artificial intelligence (AI) is going to shift the boundaries still further.

With the right balance of agility, capability, and control, you can secure your digital infrastructure, meet regulatory demands, and drive innovation on your own terms—sovereignty with purpose.

Rather than operational isolation or rejecting global cloud innovation, sovereignty with purpose is about balancing innovation, resilience, and compliance in a way that preserves autonomy, transparency, and trust.

But with the move to digital sovereignty comes risks and trade-offs. Success also demands a clear sense of what is and isn't necessary to meet your sovereignty demands. A poorly targeted and operationally restrictive approach could erode competitiveness and drive-up costs, without strengthening protection or autonomy.

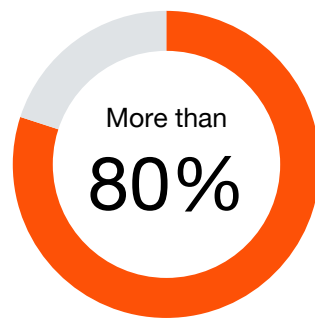
In this report, we look at how to seize the sovereignty opportunities and avoid the pitfalls as you look to balance competitiveness, resilience, and control.



01

Dealing with the fast-shifting boundaries of digital sovereignty

The rapidly growing focus on digital sovereignty is transforming cloud strategies.



More than 80% of the organisations taking part in PwC's 2025 EMEA Cloud Business Survey are refining their cloud approach in response to geopolitical and/or regulatory change. But what does digital sovereignty actually entail and why is it so critical?

Up until now, much of the focus has been on where data resides and who can access it. But as important as these considerations are, they're only scratching the surface of a far bigger strategic imperative that encompasses who controls and operates the technology and data centres, along with the evolving legal and regulatory landscape that surrounds this. You also need to determine what your organisation would do if the services upon which you depend fail or are no longer available.





The risk checklist



How much control do you have over the tech infrastructure you use?



What are the human dependencies within your tech infrastructure?



Where are the people who develop, manufacture, and support your tech infrastructure based, and who do they answer to?



How reliant are you on a single provider and what vulnerabilities does this create—if they hike up prices, for example, how quickly could you switch?



How will AI reshape your tech infrastructure and your ability to sustain sovereignty?



How quickly could you get power, connectivity, and networks back up and running if operations go down, are attacked, or are withdrawn?



What kind of legal exposures do you face—from data appropriation outside your jurisdiction to breach of contract claims if services are interrupted?

Concerns over dependencies and vulnerabilities

As organisations operate within an increasingly interconnected digital ecosystem, sovereignty considerations are becoming more prominent. These dynamics can introduce dependencies across the digital supply chain that require careful governance and oversight.

For example, organisations may need to plan for potential disruptions or evolving operating conditions linked to geopolitical or regulatory developments. Ensuring resilience across this extended supply chain is therefore becoming a key priority for many organisations.

And the factor that is often underestimated is the dependency on a narrow pool of key personnel, including the specialists who develop, manage, and maintain your systems.

AI moves the goal posts

The stakes are going to get even higher as AI moves the sovereign boundaries.

AI operates through globally dispersed and rapidly evolving models and data pipelines, which can make it harder to maintain visibility or control. While AI offers considerable benefits, it could therefore add a further layer of complexity to the challenge of maintaining effective governance and transparency over transnational technology supply chains and data flows. The key question is no longer where the data is located, but where it's processed and where and how the outputs are inferred and applied.

Intensifying regulatory spotlight

As concerns over autonomy and protection mount, policymakers, and regulators across EMEA are sharpening their focus on digital sovereignty.

Alongside the far-reaching General Data Protection Regulation (GDPR) provisions, a growing array of sovereign-related compliance demands now includes the EU AI Act, safeguarding of critical national infrastructure as part of the EU NIS-2, and operational resilience requirements under the EU Digital Operational Resilience Act (DORA).

The most stringent sovereignty regulations centre on national security or sectors entrusted with sensitive personal data such as health, financial services, and public services. For example, guarding against cloud service disruption and other third-party risks is a key pillar of DORA for financial services.

Complying with these requirements is clearly an important part of your licence to operate. But regulations tend to trail behind today's fast-changing geopolitical, technological, and market realities. The bigger questions are: what does sovereignty mean for your unique organisation, how does it align with your business objectives, and what cloud strategies and governance structures do you need to meet these demands.



Licence to transform

Sovereignty isn't just a priority for highly regulated industries. As the cloud becomes the primary springboard for transformation across the economy, digital sovereignty offers operational continuity and control. The results would enable you to harness new technologies with confidence and assurance.



Digital sovereignty is a complex and fast-evolving business imperative. With organisations' ability to operate and compete at stake, there's an urgent need to identify the sovereignty risks they face, what the risk appetite is, and have a clear plan on how to secure and sustain the technology upon which they depend.

Nicola Quincey

Partner, EMEA AWS Alliance Leader, PwC UK





02

Making the right choice for your organisation

The complexities of digital sovereignty are shaping the cloud choices facing your organisation. Each cloud operating model has pros and cons, though some of the perceived advantages may not be as clear-cut as is often assumed.

Private on-premises cloud

By managing data and operations in-house, a private on-premises cloud might look like it offers the greatest level of security and control. But the need to develop and manage your own cloud services could ramp up development and operating costs. Lack of data centre back-up could also heighten resilience challenges.

Further questions centre on whether in-house functionality and scalability could be developed and implemented fast enough to keep pace with advances in areas such as AI.

It's also important to factor in limited data centre capacity and dependence on a small number of key personnel. The results could heighten your vulnerability to outages without the safety net of data portability and operational back-up.

National cloud

Opting for a domestically owned and operated national cloud service would ensure that data stays within national boundaries. National clouds may effectively service local demand, but for organisations operating across jurisdictions, they may not meet performance and latency requirements. By partnering with global cloud service providers (CSPs), this model can open up access to at least some public cloud functionality, helping organisations retain control without compromise.

However, the limited number of in-country data centres creates a concentration risk that could leave your organisation dangerously exposed if the service is attacked or goes down.

Sovereign-by-design

The need to balance functionality, security, and autonomy is becoming table stakes for public sector and regulated industries that are concerned about retaining control and agency over their technology and infrastructure investments.

The AWS Cloud is secure and sovereign-by-design and has been so from day one, providing a comprehensive set of technical measures, operational controls, and contractual protections that give customers control over where they locate their data, who can access it, and how it is used.

This commitment is reflected in the AWS Nitro System, which provides a strong physical and logical security boundary. It is designed to enforce restrictions so that nobody—including anyone at AWS—can access customer workloads on EC2, even to fulfill a law enforcement request.

These services are available across all 39 AWS Regions; each Region has multiple redundant, fault-isolated Availability Zones. AWS supports 143 security standards and compliance certifications, and customers can directly inherit controls to help comply with local laws and regulations.

Critically, AWS extends the same infrastructure, services, APIs, and tools beyond its Regions to wherever customers need them, delivering a consistent experience regardless of deployment location. Whether through AWS Outposts on customer premises, AWS Dedicated Local Zones built for the exclusive use of a single customer or community, or AWS AI Factories, which bring fully managed AI training and inference infrastructure directly into customer data centres. This continuum of infrastructure options gives customers the flexibility to address stringent data residency, isolation, and in-country processing requirements while remaining on a single, unified platform with no need to rearchitect, retool, or retrain, thus giving customers control without compromise.

The recently launched AWS European Sovereign Cloud extends customer choice by offering the same security, availability, and performance that customers expect from existing AWS Regions.

It offers the full power of the AWS Cloud, with a comprehensive and familiar service portfolio, architecture, and APIs — operated exclusively by EU residents, with no critical dependencies on non-EU resident infrastructure, enabling it to continue operating indefinitely even when disconnected from the rest of the world. This gives customers more control, with all customer content and customer-generated metadata retained locally, alongside increased resilience options between global AWS Regions and the AWS European Sovereign Cloud Region.

A dedicated governance structure underpins the cloud, including a new parent company incorporated in Germany, led by EU citizens, obligated to comply with European laws and act in the best interests of the AWS European Sovereign Cloud. Governance oversight is further supported by an advisory board that includes independent members, all of whom are European citizens and residents, ensuring transparency.

These defining features underpin a fully featured cloud with over 100 services, supported by more than 160 launch partners, giving customers the choice and agency to innovate without compromising their sovereign control.



Customers want the best of both worlds—they want to be able to use the full power of the cloud and AI services, while ensuring they can meet their stringent sovereignty requirements. AWS is sovereign-by-design and we continue to invent to provide customers with more choice and control. By building a new cloud that is European in its infrastructure, operations, and governance, we're empowering organisations to innovate with confidence, while maintaining complete control over their digital assets. We're looking forward to how the expansion of AWS innovation across Europe will help supercharge customers' growth and AI ambitions.

Stéphane Israël

Managing Director of the AWS European Sovereign Cloud and Digital Sovereignty, AWS



“

In the past, organisations would have faced a straight choice between sovereignty and functionality. But it's now possible to choose from a sliding scale of options. Within the public cloud, sovereign controls can now include data residency, data encryption, and control over who has access to that data. Solutions like AWS European Sovereign Cloud take this further by adding operational sovereignty to the data controls, while still being able to provide most of the features available on the public cloud.

Johnny Chivers

Director, EMEA AWS Alliance CTO, PwC UK

Judging the right path for your organisation

This new generation of sovereign solutions means that sovereignty and innovation no longer need to pull in opposite directions.

But the complexities remain. There is no silver bullet or one-size-fits-all solution when you need to meet so many organisation-specific demands. Solutions have to take account of factors ranging from your AI and innovation ambitions, cloud computing requirements, and multi-jurisdictional regulatory obligations to the maturity of your tech estate and the nature of your existing vendor relationships, as well as cloud business continuity, auditability, compliance, supply chain resilience, and interoperability considerations.

In practice, the way forward is likely to require a series of decisions that need to be carefully evaluated and balanced, depending on your sovereignty demands and underlying risk appetite and organisational goals.



For example, you might want to outsource some of the threat intelligence, cyber security, and business continuity measures you need to protect your organisation to a cloud provider with the strength in depth to deliver. The price would be placing some aspects of your resilience strategy in the hands of specialists operating beyond your territorial borders.

The AWS Cloud can address these trade-offs, ensuring customers retain sovereign control over their technology and infrastructure investments without compromising their ability to modernise, innovate, and accelerate time to market.

Solutions like AWS European Sovereign Cloud can help address these needs by offering controls over data and operational sovereignty beyond those available in the public cloud.

Within this broader AWS Cloud approach, options such as AWS Outposts, AWS Dedicated Local Zones, and AWS AI Factories extend sovereign control and provide customers with additional deployment choices, rather than being positioned as direct alternatives to AWS European Sovereign Cloud.

These options are particularly relevant for customers with more stringent isolation and in-country data residency requirements, enabling them to deploy AWS European Sovereign Cloud infrastructure in locations aligned to their needs. Organisations can therefore select capabilities based on their specific operational, regulatory, and innovation requirements.

You may choose to operate with a combination of public, national, private, or sovereign cloud options depending on the criticality and regulatory requirements for particular types of data and workload. However, these decisions can be complicated by the extent to which data and workloads can be both critical and require innovative technology, with the move to AI increasing the intersection between these dual demands.





03

Five steps to digital sovereignty

How can you meet today's increasingly complex sovereignty demands and balance the necessary trade-offs this entails? Five priorities stand out:

01

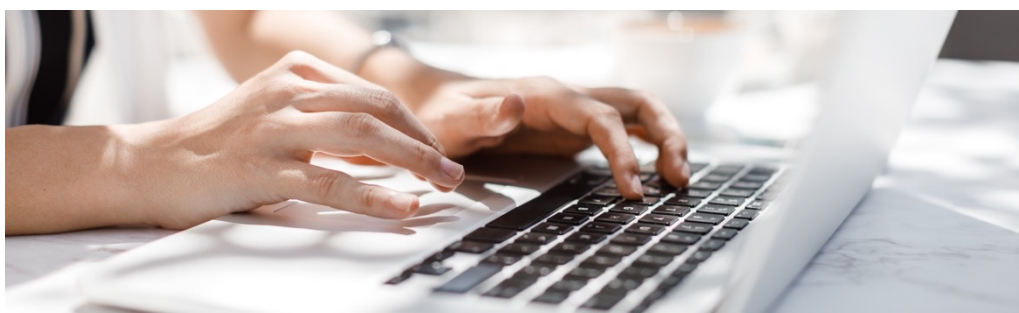
Judge what sovereignty means for your organisation

The starting point is creating a definition of sovereignty and the objectives it needs to achieve that are relevant to your organisation as a whole and to specific areas within it.

What are your regulatory obligations? How much third-party risk and dependency are you prepared to accept as you look to accelerate innovation and take advantage of advancing cloud capabilities? How much financial cost and potential disruption are you prepared to bear to meet your sovereignty goals?

With this definition in place, you can begin to judge what kind of sovereign solution or solutions would best meet your business needs and tailor this to your risk appetite and strategic goals.

Clarity over your objectives will also help you to judge how far you want to go. For example, would you want to commit to a fully sovereign solution when other options could deliver most of the same specifications with fewer drawbacks in terms of cost, disruption, and operational limitation?





“

Digital sovereignty is first and foremost a business issue. So key evaluations and decisions shouldn't be left to technical teams to deal with on their own. The people who should be making these calls are the leaders who understand the business risks and where to draw the lines.

James Rashleigh

Partner, EMEA Cyber Leader, PwC UK



Strategic checklist

Your sovereignty strategy and model choices are specific to your organisation. A number of foundational questions can provide a useful starting point for evaluation:

- ☐ What level of sovereignty do you require to meet your strategic goals and regulatory requirements—and what's optional?
- ☐ How do you balance innovation and compliance without creating unnecessary complexity or cost?
- ☐ What's the right level of shared responsibility between you, your cloud provider, and strategic partners?
- ☐ How can you future-proof your cloud strategy to take account of evolving regulations and geopolitical uncertainties?

02

Embed sovereignty into your cloud strategy from the outset

Digital sovereignty needs to be built into cloud plans and their implementation from the beginning of the design stage. If it's left to the implementation phase or missed altogether, unforeseen gaps can often emerge in areas ranging from access control to regulatory compliance.

Practical considerations include securing sufficient data centre capacity. With the move to sovereign solutions gathering pace, space in local and regional data centres is going to be at a premium.



Looking ahead, the key challenge is future-proofing your sovereignty strategy to take account of AI. The need to strike the right balance between innovation, speed, and control cuts across multiple layers and dimensions of AI sovereignty right through from model development through to deployment and governance. Areas of focus stretch from energy demands and processing infrastructure to data residency, technological dependencies, and ethical and responsible use.

03

Align sovereignty and cyber security

Digital sovereignty and cyber security go hand in hand. Close alignment can help your organisation to innovate with confidence, safe in the knowledge that access to data, tech dependencies, and other key resilience priorities are appropriately controlled.

Underlining the importance of sovereignty in your cyber strategy, data compliance, residency, and control feature strongly in the information security management ISO 27001.

Sovereignty-related security priorities include the design and development of architectures that allow you to keep sensitive data and critical tech capabilities within controlled environments, while using full-feature public clouds for other workloads.

It's also important to recognise the close interactions between data protection and third-party risks in regulations like DORA and NIS-2.





04

Recognise the human dimension

This includes training the specialists needed to drive innovation, ease key person dependencies, and boost digital autonomy.

The human dimension also encompasses workforce skills and buy-in. The starting point is articulating a clear and convincing case for why sovereignty is strategically critical and the benefits it delivers. Further considerations include the need for new ways of working within a sovereign environment, especially when teams are accessing data and using technology across hybrid multi-cloud infrastructure.



05

Bring in a trusted partner

These are complex strategic considerations, with commercial and organisational as well as technological implications.

Advice and support from a trusted partner can help you to balance all the different considerations and deliver the right sovereign solution for your organisation, from design through to implementation and managed service execution.

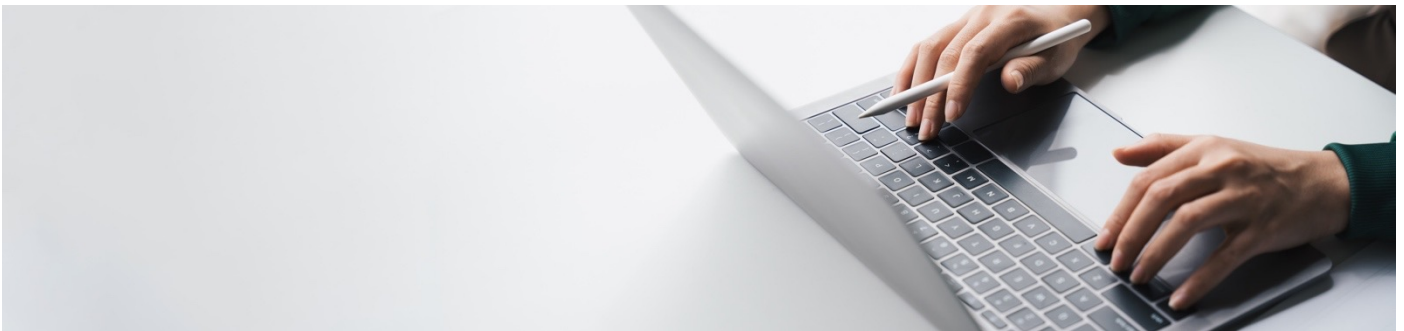
This is where we at PwC can help make the difference. By bringing together tech expertise with a deep understanding of your market, regulatory environment, and risk landscape, we're ideally placed to help you to define what sovereignty means to your organisation, the compliance requirements you need to meet, how associated risks can be managed, and how these align with your transformation and wider organisational goals.

Building on this strategic assessment, we can help you to identify the sovereignty solution that will enable you to achieve your objectives, weigh up the risks and opportunities, and manage the trade-offs.

By working with AWS and using their end-to-end cloud capabilities, we can deliver a future-proof sovereign cloud strategy and see it through to execution. Our deep technical and implementation expertise is reflected in our status as a verified [AWS Digital Sovereignty Competency Partner](#) for AWS European Sovereign Cloud.

As part of an all-round solution, we don't just focus on the sovereign engineering and architecture, but also on developing governance frameworks and in-house know-how and buy-in. And to make sure your solution is meeting demands, we carry out assurance evaluations and develop action plans to address identified gaps.

We can not only help you assess what AWS European Sovereign Cloud and the broader AWS Cloud offer, but also how to design the surrounding control environment, operating model, and governance framework. That's often the key differentiator between basic cloud adoption and a resilient, business-driven sovereignty strategy.



Capabilities available across the AWS Cloud, including the AWS European Sovereign Cloud, are among the options we would explore as we look to design and build the right solution for your organisation.

When looking at different cloud approaches, we don't just help you to understand the offerings, but how to design the surrounding control environment, operating model, and governance framework.



Conclusion:

Future-ready sovereignty

Digital sovereignty will continue to evolve at pace, with new demands, solutions, and opportunities coming to the fore.

As AI moves up the strategic agenda, greater focus is being placed on how AI software is developed, operated, and maintained, and how organisations retain control and agency over its use. Managed infrastructure options such as [AWS AI Factories](#) provide a secure and fully managed infrastructure, which you can deploy in your own data centres. As you look to combine innovation with security, this approach allows you to train and run your AI models on proprietary data while meeting strict regulatory requirements for where data is processed and stored.

The need for customisation is also seeing the emergence of industry-focused sovereign solutions for sectors with highly specific demands such as government, financial services, and health and life sciences. Further developments on the horizon include sovereign digital ecosystems, which provide local partner solutions with EU-controlled operations.

As sovereignty matures, it's set to become a cloud design principle, embedded early in strategies rather than being added later or retrofitted into existing capabilities. We're also likely to see greater standardisation and clarification of sovereignty requirements at an EU level, with greater focus on operational resilience, crisis readiness, and survivability.

As boards take the lead, any data or tech isolationism will give way to a more pragmatic business-led approach. The key priority is using global CSPs responsibly. That means putting the right governance, transparency, and control mechanisms in place.

With digital sovereignty cemented and embedded, your organisation will be in a stronger position to accelerate transformation and innovate with confidence. At a national and regional level, this is an opportunity to develop the skills and the capabilities needed to drive economic development and competitiveness.



Market spotlights



France



Germany



Italy



Middle East



UK



Spotlight on France

Sovereignty priorities

- National control over critical data and infrastructure
- Hybrid and multi-cloud strategies dominate

Key regulations

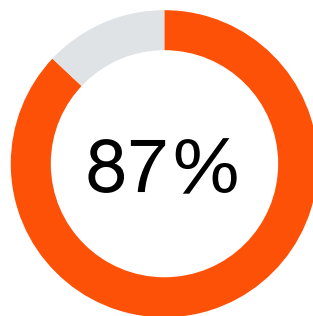
- Localisation of data handling, residency, and operational control under the SecNumCloud certification
- Military Programming Law (LPM) mandates cybersecurity and resilience standards. The LPM not only covers defence industries, but also other 'organisations of vital importance' in areas such as energy, transport, telecommunications, and health
- NIS-2 is expanding the scope of regulated entities and increasing security obligations, with a convergence underway between French regulatory frameworks, NIS-2, and SecNumCloud

Key developments

- Launch of AWS European Sovereign Cloud. Sovereignty benefits include data residency and operational control within the EU

The evolving sovereignty agenda

Cloud adoption is highly advanced in France in line with the country's 'cloud first' policy.



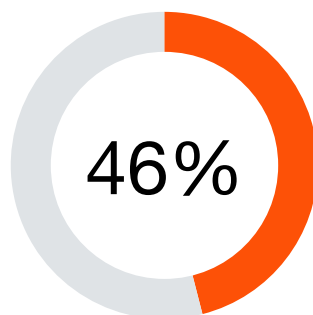
87% of organisations in France have largely or fully embraced cloud technologies, compared to 80% for the rest of EMEA

Source:

PwC's 2025 EMEA Cloud Business Survey



The regulatory focus on data residency, operational resilience and tech autonomy is increasing. Also high on the agenda is protection against legal risks such as extraterritorial access to private data.



46% of French organisations cite AI as the main reason for adopting a sovereign cloud (versus 30% in EMEA as a whole), showing that sovereignty is seen as a lever for innovation, not a constraint

Source:

PwC's 2025 EMEA Cloud Business Survey

Assessing the sovereignty options

The balance between innovation and sovereignty requires trade-offs, which will influence the choice and positioning of the sovereign cloud solution.

Alongside public and private cloud options, customers in France can now deploy national cloud solutions. These allow your organisation to use some of the capabilities developed by global CSPs, while operating within a locally owned and hosted platform.

Sovereign cloud solutions take competitiveness and control to the next level. While offering strict isolation within geographical boundaries, AWS Region covering France consists of three, isolated, and physically separate data centres (Availability Zones).



To ensure residency and autonomy, the sovereign cloud still comes with some restrictions and trade-offs when compared to the full-blown capacity and functionality of a public cloud. But sovereign cloud solutions still offer the speed, agility, and access to existing innovations you need to stay in the game.

Nicolas Barbier

Director, Cloud Solutions Architect, PwC France and Maghreb

Delivering your sovereignty strategy

The right cloud solution aligns business, compliance, and technological considerations.

Our team at PwC works closely with clients to help them understand their sovereignty requirements, build them into their tech architecture, and align these with their organisational goals.

Our combination of market, regulatory, and tech expertise can be especially valuable in helping organisations to translate their strategy into a clear set of deliverable priorities. Our ability to help clients align sovereignty and cyber security is demonstrated by our ANSSI accreditation.





Spotlight on Germany

Sovereignty priorities

- Data protection and privacy
- Industry-specific regulation including the public sector, financial services, healthcare, and critical infrastructure
- Operational control as organisations seek to limit extraterritorial access and political influence

Key regulations

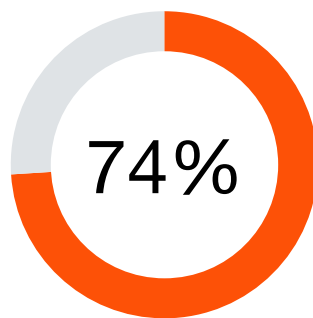
- Cloud forms part of the critical infrastructure (KRITIS) regulations on protection and resilience
- NIS-2
- EU AI Act
- GDPR

Key developments

- Launch of AWS European Sovereign Cloud, which is governed and operated from Germany and is physically and logically independent from other AWS Regions. Sovereignty benefits include data residency and operational control within the EU

The evolving sovereignty agenda

The move to the cloud has accelerated innovation and digital transformation. But policymakers and regulators have become increasingly concerned about extraterritorial access to German data and the country's growing dependence on technology developed, owned, and run outside the EU.



74% of organisations in Germany have largely or fully embraced cloud technologies, positioning themselves to leverage innovation and scalability

Source:

PwC's 2025 EMEA Cloud Business Survey



Assessing the sovereignty options

Growing demand for digital sovereignty has led to the development of a range of new and evolving solutions.



By moving beyond isolation and rejection of global cloud capabilities, the emergence of a new generation of sovereign solutions is an opportunity to balance innovation, resilience, and compliance in a way that preserves autonomy, transparency, and trust.

Hauke Schaettiger

Partner, Cloud Leader, PwC Germany

The choice includes national cloud services which are owned and operated from within Germany. These fit well with policymakers' push to develop domestic capabilities and protect data from outside interference. The big drawback is the lack of scale. With only a few data centres in operation, it can be difficult to get back up and running if facilities break down or come under attack.

AWS European Sovereign Cloud, which is now available in Germany, further enhances the sovereign options. Data residency and operational control remain within the EU. The Germany-headquartered European Sovereign Cloud is also staffed and run by EU-based personnel. The German Federal Office for Information Security (BSI) has been supporting AWS in designing the security and sovereignty features of its European Sovereign Cloud.

Delivering your sovereignty strategy

From a strategic perspective, key questions include what level of sovereignty your organisation requires to meet its business and regulatory demands—and what's optional.



As a trusted advisor and independent cloud transformation partner, we at PwC can help you to balance all these different considerations and deliver the right solution for your organisation, while curbing needless complexity and costs.

We understand how sovereignty requirements differ across sectors and jurisdictions, and how regulators interpret them in practice.



Spotlight on Italy

Sovereignty priorities

- Protecting digital infrastructure and data from extraterritorial influence
- The creation of national data centres to ensure public data is stored securely within the country
- Developing home-grown tech capabilities
- Ensuring operational resilience and business continuity for critical services
- Maintaining control over data access, encryption keys, and cloud operations

Key regulations

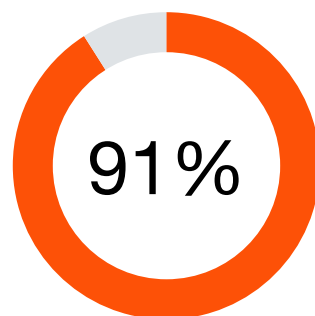
- NIS-2
- EU AI Act
- GDPR
- Digital operational resilience act (DORA)

Key developments

- AWS is investing more than €1.2 billion to expand its cloud infrastructure and services in Italy's AWS Europe (Milan) Region.

The evolving sovereignty agenda

Migration to the cloud is among the highest in EMEA, driven by AI adoption and modernisation of legacy systems.



91% of organisations in Italy have largely embraced cloud technologies, including almost one third which already run all of their operations in the cloud

Source:

PwC's 2025 EMEA Cloud Business Survey

Sovereignty has emerged as a key priority for policymakers, regulators, and private and public sector organisations as they look to strengthen autonomy over critical digital assets.

This is particularly important in highly regulated sectors such as financial services, public administration, energy, and healthcare, where organisations must balance innovation with security, compliance, and operational control.



Assessing the sovereignty options

AWS European Sovereign Cloud is accessible from Italy and will further enhance the balance between innovation, compliance, and control by ensuring that data and operations remain within the EU. For Italian clients, this can provide greater confidence around residency, access restrictions, and accountability.

But sovereign infrastructure is only one part of the answer. It's also important to develop a robust operating model, clear controls, and strong governance.

Organisations also need to consider third-party risk, supply chain dependencies, identity and access management, and incident response capabilities as part of their overall sovereignty strategy.



Sovereign solutions can strengthen confidence around residency, access, and accountability. But the approach needs to be pragmatic rather than ideological. The right answer depends on the criticality of the workload, the regulatory demands, and the organisation's operational maturity. The important point is to assess sovereignty not only in terms of where data and systems are located, but also who operates them, who holds the keys, and how to ensure resilience if threats materialise.

Nicola Sfondrini

Partner, Cloud Infrastructure, PwC Italy

Delivering your sovereignty strategy

With the sovereignty opportunities come practical challenges. These include determining which workloads require specific protections and what level of sovereignty is necessary as you look to reconcile compliance with efficiency and innovation.

This is where the strategic advice and implementation support offered by PwC can be so valuable. We can help your organisation to translate broad business objectives and regulatory demands into concrete architecture, governance, and sourcing decisions.



When looking at different cloud solutions, we don't just help organisations to understand what the platform offers, but how to design the surrounding control environment, operating model, and governance framework. That is often the real differentiator between simple cloud adoption and a resilient sovereignty strategy.

We also help organisations define data classification models, sovereignty requirements by workload, and practical governance frameworks that enable consistent decision-making across hybrid and multi-cloud environments.



Spotlight on Middle East

Sovereignty priorities

- National control over critical data and infrastructure
- Protection of critical digital assets

Key regulations

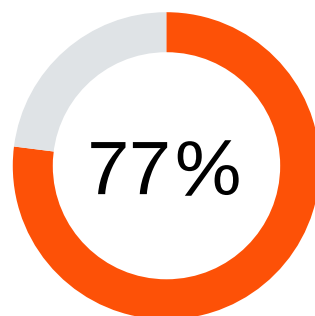
- [Saudi Arabia Personal Data Protection Law](#)
- United Arab Emirates (UAE) Personal Data Protection Law
- [Qatar Personal Data Privacy Protection Law](#)
- Cyber standards from Saudi Arabia's National Cybersecurity Authority (NCA), Qatar's National Cyber Security Agency (NCSA) and the UAE's Information Assurance (IA) regulation

Key developments

- [AWS Public Regions](#) exist in Bahrain, Israel, UAE, and are coming soon to Saudi Arabia. A local zone exists in Oman.
- [AWS Outposts](#) rack is now supported in the AWS Middle East (UAE) and the AWS Israel (Tel Aviv) Regions

The evolving sovereignty agenda

Cloud adoption across the Middle East is accelerating, driven by national digital agendas and strong government sponsorship.



77% of organisations in the Middle East have largely or fully embraced cloud technologies

Source:

PwC's 2025 EMEA Cloud Business Survey

A combination of regional tensions and the need for security, isolation, and compliance have heightened the focus on sovereignty in sectors like government, financial services, energy, and healthcare.

While data privacy remains an important consideration, sovereignty priorities in the Middle East are often more strongly shaped by national resilience, operational control, and strategic autonomy, with the balance varying by country, sector, and regulatory context.

One of the key challenges is the need to balance data, operational, and technological sovereignty. Keeping data and infrastructure under national control can impede portability and survivability in the event of outages or attacks.





With so much focus on data and operational sovereignty, organisations shouldn't lose sight of the equally critical technological sovereignty. To sustain resilience in a heightened threat environment and avoid vendor lock-in, it's important to make sure that workloads are portable and interoperable across cloud environments.

Nikolaos Lioulis

Principal, Strategy&, Middle East

Assessing the sovereignty options

It's important to assess sovereignty options based on four factors: workload criticality, regulatory sensitivity, resilience requirements, and the need for access to advanced cloud and AI capabilities.

Private on-premises environments may be appropriate for the most sensitive workloads requiring maximum control but can limit scalability and access to innovation.

Hybrid and multi-cloud models can help address diverse business and regulatory needs, although they can increase operational complexity.

Where available, sovereign cloud solutions such as AWS dedicated local zones and AWS Outposts can offer a more balanced model by combining enhanced control and compliance with access to public cloud capabilities.

In the Middle East, sovereign cloud is not only a compliance response. It's increasingly part of a broader national digital strategy. Key aims include strengthening continuity of critical services, reducing dependency in strategically important digital domains, and enabling governments and regulated sectors to scale advanced digital and AI capabilities with greater confidence and control.



Hybrid private and public cloud solutions can no longer provide a satisfactory answer as AI blurs the lines between innovation critical and highly regulated data and workloads. Sovereign cloud solutions can provide a better answer to these dual demands by adding an extra layer of compliance and control to public cloud capabilities.

Achilles Drettas

Partner, Strategy&, Middle East



Delivering your sovereignty strategy

At PwC, we recognise that your sovereignty strategy is a business rather than just tech priority, with a crucial impact on your ability to transform and compete. Our advice and support are designed to help you strike the right balance between innovation, compliance, and control.

Our relationships with regulators and cloud service providers mean that we can help clients understand what can often be nuanced demands and judge the right solution for their particular organisation. Key steps include helping you to manage workload segmentation, customise your technology architecture, and build this into a future-fit operating model.





Spotlight on UK

Sovereignty priorities

- Data protection and privacy
- Development of digital skills and technology
- National Cyber Security Centre's focus on resilience

Key regulations

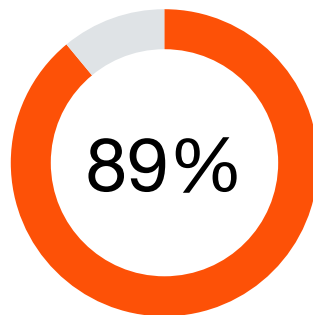
- Close alignment with EU regulations including the UK GDPR and DORA
- National Security and Investment Act gives the government powers to intervene in acquisitions of tech firms that could pose security risks

Key developments

- The UK Government's Modern Industrial Strategy and the accompanying Digital and Technologies Sector Plan promote the development of sovereign capabilities in key technologies like AI and cloud computing

The evolving sovereignty agenda

Cloud adoption in the UK is highly advanced. But the business and regulatory focus on digital sovereignty has until recently been less prominent than other major European markets.



89% of organisations in the UK have largely or fully embraced cloud technologies.

Source:

PwC's 2025 EMEA Cloud Business Survey

But geopolitical tensions are now shifting the sovereignty conversation from a theoretical evaluation to the development of concrete action plans.

The growing threat from cyberattacks has sharpened the focus on digital resilience and survivability.





“

If organisations distil down resilience, the overriding priority is being able to respond effectively and at pace in a crisis scenario. From a sovereignty perspective, the key focus is how to recover tech estates or switch to other territories and providers if services are compromised or go down. The challenges that need to be addressed include how to strengthen portability and recoverability while meeting regulatory and national security demands to keep data within the country.

Karen Penman

Partner, Digital and Cyber Resilience Leader, PwC UK

Amid uncertainties over trading relationships, further concerns centre on the risk of tariff-driven price hikes for cloud services. More services provided and controlled locally would help to ease the risks.

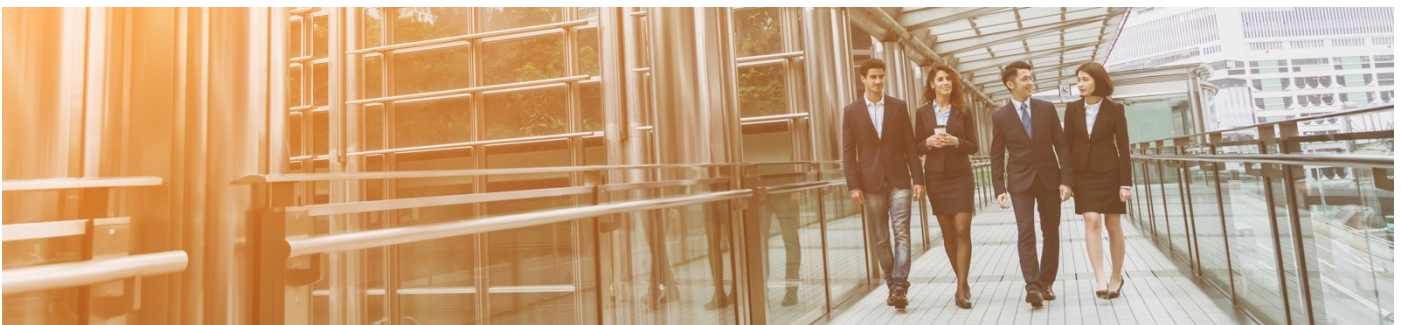
With backing from the UK government, digital sovereignty is also an opportunity to accelerate the development of skills and technology within the UK.

Assessing the sovereignty options

The threats to critical digital infrastructure are increasing the demand for sovereignty by design and closely related resilience by design.

Global cloud service providers like AWS have been stepping up investment in the development of data centres and other infrastructure within the UK. AWS UK public region combines data isolation within defined geographical boundaries with the functionality and scalability of a global CSP.

As sovereignty moves from theoretical risk to business reality, the key question for organisations is what are they trying to protect and what level of risk are they prepared to accept.



Delivering your sovereignty strategy

Drawing on our industry, regulatory, and tech expertise, we're helping a range of organisations to design and implement sovereign solutions that balance the different and potentially competing priorities.

We look at sovereignty from a range of perspectives including regulation, cost, and resilience, all with the ultimate aim of strengthening control and trust—sovereignty with purpose.

Authors



Stéphane Israël

Managing Director of
the AWS European Sovereign Cloud
and Digital Sovereignty,
AWS



Achilles Drettas

Partner,
Strategy&,
Middle East



Hauke Schaettiger

Partner,
Cloud Leader,
PwC Germany



James Rashleigh

Partner,
EMEA Cyber Leader,
PwC UK



Karen Penman

Partner,
Digital and
Cyber Resilience Leader,
PwC UK



Nicola Quincey

Partner,
EMEA AWS Alliance Leader,
PwC UK



Nicola Sfondrini

Partner,
Cloud Infrastructure,
PwC Italy



Nikolaos Lioulis

Principal,
Strategy&,
Middle East



Johnny Chivers

Director,
EMEA AWS Alliance CTO,
PwC UK



Nicolas Barbier

Director,
Cloud Solutions Architect,
PwC France and Maghreb

