

SOVEREIGN CLOUD TECHNOLOGIES

IS THE CLOUD REALLY JUST SOMEBODY ELSE'S COMPUTER?

"Cloud is about how you do computing, not where you do computing."

Paul Maritz, former CEO of VMware.

"I don't need a hard disk in my computer if I can get to the server faster... carrying around these non-connected computers is byzantine by comparison."

Steve Jobs, Co-founder, CEO and Chairman of Apple

INTRODUCTION

Cloud computing, the long-held dream of computing as a utility, has already transformed how a very large segment of businesses and organisations work, communicate, and collaborate, and is fast becoming a necessity to stay competitive in today's digital world, making software even more attractive as a service and shaping the way IT software and hardware is designed and purchased.

Moving to the cloud is giving organisations of all shapes and sizes the ability to move faster, be more agile, and innovate their products and services. IT service providers need not be concerned about over-provisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or under-provisioning for one that becomes wildly popular, thus sacrificing the quality of their service. This elasticity of resources provided by cloud computing technology is unprecedented in the history of IT. Although cloud technologies have been widely used, discussed and researched for at least two decades, some confusion remains about exactly what the cloud is and when it is useful.

For any organisation considering moving to cloud-based services and solutions, it is not only important to understand the basics of cloud computing and how it can help to accelerate its digital transformation, but also the advantages and limitations of this thriving yet quite young technology.

WHAT IS CLOUD COMPUTING?

Although the origins of cloud computing can be dated back to the early 1960s, the concept as we know it today emerged in the 1990s as a new computing paradigm which aims to provide computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services.

Such new computing strategy was born as an alternative to the traditional 'on-premises' computing environment, where an organisation runs and manages its own hardware, software, data storage and other computing resources at its own physical location.

So far, no generally applicable definition for the term cloud computing has gained full acceptance. In publications, definitions are frequently used that are similar in most cases, but which still have some variations from one to another. The International Organisation for Standardization (ISO) has defined cloud computing in its dedicated standard as¹:

"Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand".

In the previous definition: 'resources' include, for instance, servers, operating systems, networks, software applications and storage equipment.

¹ ISO/IEC 22123-2:2023 – Cloud computing – Part 2: Concepts

In the same ISO definition, 'self-service provisioning' refers to the provisioning of resources for cloud services that the cloud customers carry out with the help of automated means. Where a cloud service is an information technology service offered as part of cloud computing, including, among others, infrastructure, platforms and software.

In essence, cloud computing is a transformative technology that enables access to shared pools of configurable IT resources (e.g., servers, storage, databases, and applications) over the internet. These resources are managed by cloud service providers (CSPs), allowing users to access services remotely without needing extensive on-premises infrastructure. In other words, this approach provides the possibility for organisations to manage in a more efficient way their hardware and software infrastructure, offering flexibility, scalability, and cost-efficiency.

WHAT ARE THE KEY CHARACTERISTICS OF CLOUD COMPUTING?

In 2011, in their official definition of cloud computing², the US NIST (National Institute for Standard and Technology) provided a list of five key characteristics for this new technology. Since then, these five points have been increased to six by the latest version of the ISO/IEC 22123 standard published in 2023:



Broad network access: Services are available over a network using standard mechanisms (e.g., mobile phones, tablets, laptops or workstations) and are not tied to a specific client.



Measured service: Resource usage can be measured, monitored and metered accordingly (examples of measured resources are: storage, processing, bandwidth, user

accounts). It can be therefore made available to cloud customers, providing transparency for both the provider and consumer of the utilized service.



Multi-tenancy: Physical or virtual resources are allocated in such a way that the processes and data of different clients are separated and inaccessible to each other.



On-demand self-service: Provisioning of resources (e.g., computing power or storage) runs automatically without manual interaction from the cloud provider.



Rapid elasticity and scalability: Cloud services can be made available quickly and elastically, in some cases automatically. From the user's perspective, the resources therefore appear to be unlimited.



Resource pooling: The cloud provider's resources are available in a pool from which cloud users are served (multi-tenant model). Users do not know exactly where the resources

are located. However, they can often contractually specify the storage location, e.g., region, country or datacentre.

It is important to highlight that, as any other recent technological advancement, cloud computing is subject to constant and rapid change. Therefore, there may be cloud services for which not every characteristic fully applies. As such, we should refrain from taking an overly dogmatic view of the individual points presented above.

WHICH CLOUD DEPLOYMENT MODELS ARE AVAILABLE?


The deployment of services to the cloud is referred to as cloud migration. Cloud migration can be done through three main cloud deployment models:

PUBLIC CLOUD

Public cloud is the most common type of cloud computing deployment. It is commonly defined as computing services offered by third-party providers over the public Internet, making them available to anyone who wants to use or purchase them. These services are in general sold on-demand, allowing customers to pay only per usage for the CPU cycles, storage, or bandwidth they consume. With a public cloud, all hardware, software, and other supporting infrastructure are owned and managed by the cloud provider.

In a public cloud, the same hardware, storage, and network devices are shared with other organisations or cloud 'tenants', and access to services

² NIST SP 800-145, "The NIST definition of cloud computing", 2011



and management of the account is generally done using a web browser. Public cloud deployments are frequently used to provide web-based email, online office applications, storage, and testing and development environments.

The key advantages of public clouds can be summarised as:

Cost-effectiveness: There is no need to purchase hardware or software, and the user pays only for the service he uses, so in most cases this results in reduced costs.

Maintenance: The service provider is responsible for the maintenance so that the organisation using the public cloud does not need to address it.

Scalability: Virtually 'infinite' on-demand resources are available to meet the business needs of an organisation.

Reliability: A vast network of servers ensures a very high resilience against failure and potential attacks.

PRIVATE CLOUD

In this deployment model, all resources are isolated and the cloud infrastructure is operated solely for a single organisation. It can be managed by the institution itself or by a third party and can be located in the institution's own datacentre or at the premises of a third party. In essence, in a private cloud, the hardware and software are dedicated solely to an individual organisation.

In this way, a private cloud can make it easier for an organisation to customize its resources to meet specific IT requirements. Private clouds are often used by government agencies, financial institutions, or any other mid- to large-size organisations with business-critical operations seeking enhanced control over their environment.

From a high-level perspective, the advantages of a private cloud can be summarised as:

Flexibility: An organisation using the private cloud can customize its cloud environment to meet specific business needs.

Control: Resources are not shared with others, so higher levels of control and privacy are possible.

Scalability: Private clouds often offer more scalability compared to on-premises infrastructure.

It should be noted that there is a fine line separating a private cloud deployment model and a traditional on-premises infrastructure. The two models basically differ in that, while both reside within a controlled environment, a private cloud offers the advantages of cloud computing (including scalability, automation, and resource efficiency) whereas on-premises infrastructure represents a more traditional, static approach to IT resource management.

HYBRID CLOUD

This is a computing environment that combines and unifies public cloud, private cloud and on-premises infrastructure, allowing data and applications to be shared between them.

One of the main reasons for organisations to choose a hybrid cloud approach over the public cloud (or to move from a public to a hybrid model) is to meet business imperatives such as regulatory and data sovereignty requirements, taking full advantage of on-premises technology investment, or addressing low latency issues. On the other hand, organisations using private cloud deployments typically move to hybrid cloud strategies to overcome workload limitations. These organisations usually want to continue using their existing on-premises datacentre and still access the public cloud as needed. Hybrid cloud offerings allow to seamlessly switch workloads between different environments. For instance, when organisations run out of computing resources in their internal datacentre, they deploy the extra workload to external third-party cloud services.

Based on the information laid out above, the advantages of the hybrid cloud can be summarised as:

Control: Organisations using the hybrid cloud can maintain a private infrastructure for sensitive assets or workloads that require low latency.

Flexibility: Take advantage of additional resources in the public cloud when needed.

Cost-effectiveness: With the ability to scale to the public cloud, organisations incur in costs for extra computing power only when needed.

Migration: Transitioning to the hybrid cloud is usually easier as it can be done gradually, phasing in workloads over time.

CLOUD DEPLOYMENT MODELS OVERVIEW







	PUBLIC CLOUD	HYBRID CLOUD	PRIVATE CLOUD
OWNERSHIP 	Third-party providers	Combination of third-party providers and users	Organisation/user
RESOURCE SHARING 	Multi-tenant	Mix of shared and dedicated resources	Single-tenant, dedicated resources
SCALABILITY 	Highly scalable	Flexible scaling, leveraging public and private resources	Limited by dedicated infrastructures, better than purely on-premise infrastructure
SECURITY 	Managed by providers	Sensitive data in private, public for scalability	High control, customisable security
FLEXIBILITY 	Wide range of services and global reach	Balance of control and flexibility	Customised to specific needs
COST 	Pay-as-you-go, variable	Cost optimisation possible with ability to scale public cloud components	Higher upfront and maintenance costs

Figure 1: Cloud deployment models overview

Even though the previous three deployment models are the three most common cloud options, the above definitions do not cover all variants of cloud offerings, combining different of the previous concepts. Among these other cloud options, two which are lately gathering quite significant momentum are:

- The **'multi-cloud'**, term that refers to a cloud deployment model in which a customer uses public cloud services are made available by two or more cloud service providers.

- Similarly, **'poly-cloud'** refers to the use of multiple public clouds for the purpose of leveraging specific services that each provider offers. It differs from 'multi-cloud' in that it is not designed to increase flexibility, mitigate against failures and avoid vendor lock-in situations, but is rather used to allow an organisation to achieve more than what could be done with a single provider.

WHAT IS THE BEST CLOUD DEPLOYMENT MODEL?

In other words, there is not such a thing as the 'best' cloud, or a 'one-size-fit-all' type of cloud technology. Several different cloud computing models, types, and services have evolved to meet the rapidly changing technology needs of organisations.

From the three main different approaches to deploy cloud services (public, private or hybrid), which of them is the best for a given organisation depends on the business needs and restrictions of that specific organisation.

The three most important areas to examine when selecting a specific cloud model are: control (cloud management), security (especially in what pertains to protection of the data), availability and performance.

WHAT SERVICE MODELS EXIST IN CLOUD COMPUTING?

In addition to the type of cloud deployment model (public, private or hybrid) an organisation also has the flexibility to choose the service model provided through the cloud. The three main types of cloud service models include (see Fig. 2 for a quick visual comparison among them):

Infrastructure as a service (IaaS): In the case of IaaS, IT resources such as computing power, data storage devices or networks are offered as a service. A cloud customer purchases these virtualised services and builds its own software environments for internal or external use. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications. A typical use case would be a user that needs to deploy multiple software environments (developing, testing, staging, production) but does not want to (or cannot) face the high upfront cost for hardware and the usually long provisioning times for new infrastructure. In this case, the organisation may rent computing power, memory and data storage devices in the cloud, and run the different environment of its choice on it.

Platform as a service (PaaS): A PaaS provider makes an entire infrastructure available and, on the platform, offers the customer standardised interfaces which are used by services of the customer. For example, the platform can provide multi-client capability, scalability, access control, database accesses etc. as a service. The customer has no access to the underlying layers (operating system, hardware), but is able to run its own applications on the platform, for the development

of which the cloud service provider usually offers its own tools. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly also over-configuration settings for the application-hosting environment.



Software as a service (SaaS): A SaaS provides a full-application stack as a cloud service, including the maintenance and management from underlying infrastructure to application software. This category includes all offers of applications meeting the criteria of cloud computing. Examples include contact data management, financial accounting, word processing or collaboration applications. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

The term 'as a service' is also used for a number of additional offers, such as for Security as a Service, Business Process as a Service, or a Storage as a Service, so that frequently 'XaaS' is used, i.e. 'something as a service'. Most of these offers can be assigned, at least roughly, to one of the three categories above.

In addition to more operational aspects such as availability, capacity or performance, the models listed above also differ in the customer's command level over the security of the offered services. In case of IaaS, the customer has full control of the IT environment from the operating system upwards, since everything is operated within their sphere of responsibility. In case of PaaS, the customer only has control of their applications that run on the platform and, in case of SaaS, the customer practically hands over the entire control to the cloud service provider.

All the three main service categories described above (IaaS, PaaS and SaaS) are included in the portfolio of the so-called 'hyperscalers'. These are large cloud service providers (CSPs) that offer massive, scalable infrastructure and platforms to support cloud computing on a global scale. They usually operate data centres across multiple geographic regions and deliver computing power, storage, networking, and services like AI, analytics, and DevOps tools to millions of users. Some of these main players in the cloud computing landscape include well-known companies such as

COMPARISON OF CLOUD SERVICE MODELS

		On-Premise	IaaS	PaaS	SaaS
Applications		●	●	●	●
Security		●	●	●	●
Databases		●	●	●	●
Operating Systems		●	●	●	●
Virtualisation		●	●	●	●
Servers		●	●	●	●
Storage		●	●	●	●
Networking		●	●	●	●
Data Centres		●	●	●	●



Customer Managed



Provider Managed

Figure 2: Comparison of cloud service models³

Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud or Oracle Cloud Infrastructure. Even though it probably does not qualify as a 'hyperscaler' in the strict sense, at least compared to the previously referenced 'cloud giants', it is worth

mentioning also OVHcloud as the largest company offering cloud services strictly based in the EU, which may have certain advantages in terms of sovereignty compliance, as will be discussed in one of the following sections of the present brief.

³ Adapted from https://link.springer.com/chapter/10.1007/978-3-030-43198-3_2/figures/1

WHY MOVE TO THE CLOUD?

Most of the advantages of cloud computing have already been mentioned in one way or another in the previous sections. No matter which definition, deployment model or service model of cloud is used, the benefits are in general the same: When the computing and processing demand increases beyond an on-premises datacentre's capabilities, organisations can use the cloud to instantly scale capacity up or down to handle dynamic (and hard to predict) computing demand. It also allows organisations to avoid the time and cost of purchasing, installing, and maintaining additional new servers that may not always be needed, or are perhaps required only for a limited period, for instance, while developing a new application.

Advocates of cloud computing claim that this technology brings some clear value propositions with respect to traditional on-premises solutions:



Scalability and elasticity: Scalability and elasticity via dynamic ('on-demand') provisioning of resources on a fine-grained, self-service basis in near real-time, without users having

to engineer for peak loads. This gives the ability to scale up when the usage need increases or down if resources are not being used.



Availability: Availability improves with the use of multiple redundant sites, which makes well-designed cloud computing suitable for business continuity and disaster recovery.



Maintenance: Maintenance of cloud environment is easier because the data is hosted on an outside server maintained by a provider without the need to invest in datacentre hardware.

IT maintenance of cloud computing is managed and updated by the cloud service provider which should reduce the maintenance costs compared with on-premises datacentres.



Productivity: Cloud technologies usually provide an environment specifically tailored for a faster and more seamless integration of real-time collaboration tools that allow

multiple users to work on the same data from multiple platforms and devices, increasing this way cross-teams productivity and efficiency.



Multi-tenancy: It enables sharing of resources and costs across a large pool of users thus allowing for:

1) centralization of infrastructure in locations with lower costs (such as real estate, electricity, etc.); 2) peak-load capacity increases (users need not engineer and pay for the resources and equipment to meet their highest possible load-levels); 3) utilization and efficiency improvements for systems.



Environment: Cloud computing can provide some significant environmental benefits compared to traditional in-house data centres. These advantages stem from improved

energy efficiency and resource optimisation. For instance, many of the main cloud providers optimise energy use by building data centres with state-of-the-art energy-efficiency architectures and co-locating them near sources of sustainably produced energy. It should also not be neglected the impact that cloud technologies have on reducing e-waste as a result of companies requiring fewer on-premises computational infrastructure leading to reduced production and disposal of IT hardware.



AI and advanced analytics

services: Cloud computing offers the capability of significantly enhancing the availability and usability of AI-based tools by providing scalable,

on-demand access to powerful computing resources and pre-built AI services. Cloud AI-based services allow organisations to avoid a heavy investment in specialized hardware (like GPUs or TPUs) or complex infrastructure to run advanced machine learning models. Instead, cloud platforms offer ready-to-use AI capabilities enabling even small teams or public sector bodies to experiment, deploy, and iterate AI solutions rapidly and cost-effectively. Additionally, cloud-based AI services benefit from continuous updates, robust security, and compliance support, accelerating innovation while reducing technical overhead.

WHY NOT MOVE TO THE CLOUD?

Like in any other technology, there are also limitations to cloud computing. One of the most mentioned drawbacks of cloud computing is that, in most deployment models, it relies on an internet connection. Even top

cloud service providers can experience downtime due to a natural disaster or slower performance caused by an unforeseen technical issue that might impact connectivity (e.g., Tsunami in Japan in 2011, hurricane Sandy in New York in 2012, or the California wildfires as recent as 2025). An organisation could be blocked from accessing cloud services until the problem is resolved.

Other disadvantages of cloud computing include:

Vendor lock-in: Difficulty moving workloads across different cloud providers, who generally use different and non-interoperable standards, which brings the risk of getting to a vendor lock-in situation.

Control: Less control over underlying cloud infrastructure, including updates to the environment.

Security: Concerns regarding cybersecurity risks like data privacy and online threats.

Integration: Integration complexity with existing legacy systems.

Cost management: Depending on the complexity of the selected cloud approach, it can become rather elaborate to implement an efficient cost management strategy, resulting in unforeseen costs and unexpected expenses like over-provisioning or poor use of resources. This happens, for instance, when selecting multiple cloud providers or intricate hybrid setups to ensure business continuity, which, on the downside, can lead to excessive redundancy and increased pricing. In many cases, the pay-as-you go model can inflate costs with the more intensive use of the services.

Organisations can address most of these disadvantages, to some extent, by carefully evaluating cloud service providers and their service models. Many of the issues that arise when migrating to the cloud result from a lack of clear understanding about what providers offer, pricing models, and what security tasks remain the responsibility of the customer. Also, opting for more than one service provider as in the 'multi-cloud' and 'poly-cloud' models described before in the present brief is usually an advisable option, as it drastically reduces the chances of experiencing a service failure and it also helps to prevent vendor lock-in situations (although, if not very carefully planned, it can result in over-provisioning and increased costs). In addition, adding also one of the open cloud platforms available (e.g., OpenStack,

OpenNebula or Mist.io) can give more flexibility and freedom to build and accommodate to the specific needs of an organisation and to seamlessly integrate with the required services.

One should not forget that cloud migration is not, or should not be, an irreversible path. Although less common than cloud migration, the opposite process can also happen. Due to some of the limitations mentioned above, an organisation may decide to reverse cloud migration (process also known as 'cloud repatriation') and move cloud-based workloads back to on-premise infrastructures.

WHAT CHALLENGES ARE PUBLIC INSTITUTIONS FACING TO MIGRATE TO THE CLOUD?

The challenges faced by public organisations considering migrating to the cloud do not differ, for the most part, from those faced by the private sector. Public IT managers must decide if the cost savings and flexibility/scalability to be gained through shifting data and applications to the cloud are worth the trade-off with respect to the level of control and security that is ensured in on-premises infrastructure. Decision makers both in the private and public sectors are still reluctant to jump on the cloud computing bandwagon due to traditional corporate computing concerns like the security of data, reliability of service and regulatory compliance. Indeed, many public sector IT managers consider the idea of shifting data and applications to the cloud, but control, access, security, and interoperability issues will need to be resolved before their organisation can make use and benefit from this technology.

Some of the key challenges that governmental organisations are facing as they work to integrate cloud computing offerings into their IT strategies include the need for:

- Scalability;
- High reliability and minimal latency when used for critical services;
- Securing data in the cloud;
- Open standards and interoperability;
- Revising procurement practices towards more flexible approaches;
- Resolving potential regulatory issues;

- Building new capabilities within their IT workforce and onboarding new specialised professionals;
- Assessing the return on investment of cloud computing;
- Intra-governmental cloud coordination.

Many of these challenges, that are more acute in the case of public organisations, are linked to the concept of 'sovereignty'⁴. That is why, in recent years, a new concept in cloud computing has emerged to address many of the concerns of public organisations towards this technology: the sovereign cloud.

WHAT IS THE SOVEREIGN CLOUD?

If providing a unified definition for cloud computing is already difficult, finding an agreement on what the sovereign cloud is, becomes even more challenging. We could say that, essentially, there are as many sovereign cloud definitions as there are organisations requesting their implementation.

With cloud computing continuing its spread around the globe, traditional geographic boundaries like borders are no longer sufficient to protect sensitive data and resources. From a very broad perspective, the sovereign cloud can be defined as a type of cloud computing that helps organizations comply with the laws of specific regions and countries in terms of data localisation and protection, governance, and compliance (as summarised in the diagram in Figure 3). In practice, sovereign clouds:

- Ensure that data is stored and processed within a defined geographic area.
- Comply with local data protection, privacy, and cybersecurity regulations.
- Allow governments and organizations to maintain control over sensitive data, reducing dependency on foreign cloud providers.
- Promote transparency and accountability by adhering to local legal frameworks and policies.

From the points mentioned above, the foundational requirement of most sovereign cloud solutions refers to **data sovereignty**. Organisations looking for a sovereign cloud model usually require that the data stored, processed, and managed in the cloud environments is subject to the laws, regulations, and governance structures of the country or region where it resides. This entails:

Jurisdictional control: Data remains under the legal authority of the nation/region in which it is physically located, ensuring compliance with local data protection and privacy regulations.

Regulatory compliance: Organisations must adhere to specific national or regional laws governing data access, storage, and transfer, which may affect how cloud services are used.

Autonomy and governance: Entities maintain control over their data, enabling them to enforce internal policies and security measures, even when using external cloud providers.

Risk management: By ensuring data sovereignty, organisations mitigate risks related to cross-border data transfers and potential conflicts between differing legal frameworks.

In essence, data sovereignty in cloud computing ensures that an organisation's sensitive data is governed by local legal frameworks, thereby providing clarity on data ownership, control, and compliance responsibilities.

In addition to data sovereignty another key aspect of cloud sovereign models is **operational sovereignty**. It refers to an organization's ability to maintain full control over the operational aspects of its cloud environments. This includes managing, configuring, and securing cloud resources in accordance with its own policies and regulatory requirements. Key elements include:

Control over management functions: Ensuring that decision-making, configuration, and maintenance of cloud resources are conducted under the organization's authority.

Security and compliance: Implementing and enforcing security measures, monitoring, and data governance policies without external interference.

Autonomy in operations: Having the capability to respond to incidents, perform updates, and modify infrastructure as needed to align with business and regulatory objectives.

Ensuring operational sovereignty an organisation can govern its cloud operations as if they were on-premises, while still benefiting from cloud computing's flexibility and scalability.

⁴ From a wide perspective, sovereignty is generally understood as the power or authority of governing oneself without external interference. In the case of a state, this includes the ability to make laws, enforce policies, control borders, and manage internal and external affairs.

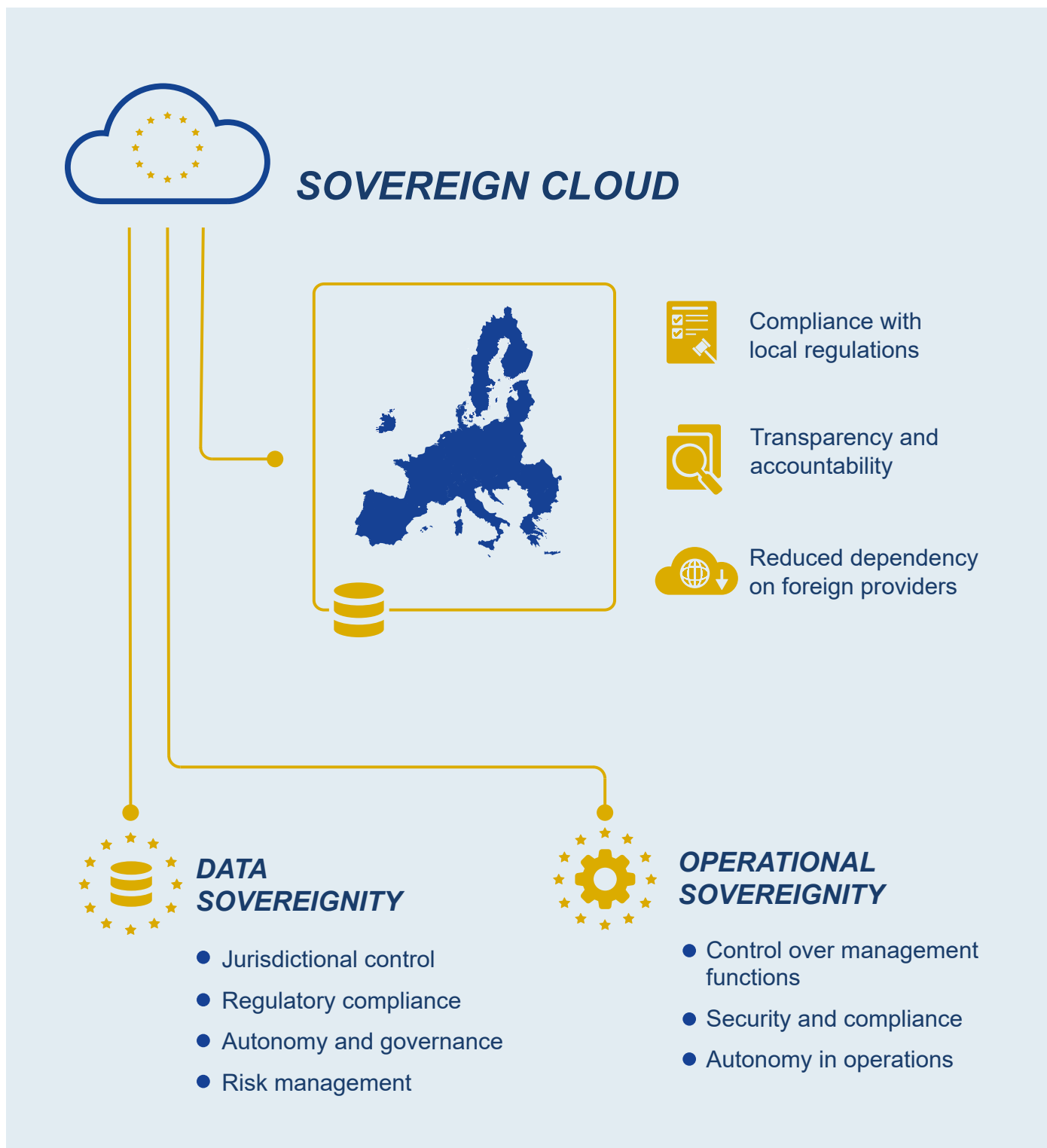


Figure 3: Diagram showing key features of a sovereign cloud

While data sovereignty and operational sovereignty remain two of the pillars of most sovereign cloud environments, since regulations around cloud technologies, and especially in what concerns to data protection, vary significantly between specific countries and regions, there is no single, accepted definition of how a sovereign cloud should operate. Approaches tend to vary by type of organisation, location and business need.

It is nonetheless true that the sovereign approach to cloud computing is becoming increasingly relevant for entities dealing with critical or sensitive information, such as public administrations, financial institutions, and organisations operating in highly regulated sectors.

WHAT IS THE EU REGULATORY LANDSCAPE FOR CLOUD COMPUTING?

As part of its digital strategy⁵, the EU aims to provide European businesses and public authorities with access to secure, sustainable and interoperable cloud infrastructures and services, including safe data storage and transmission. With this goal in mind, the European Commission (EC) strives to provide the necessary regulatory framework to ensure a safe, secure and fair cloud domain.

Given the wide variety of technologies that cloud computing relies on, the EU regulatory landscape impacting the field is a rather complex one. The different policies that govern cloud services at EU level focus mainly on data protection (including data sharing/transfer) and cybersecurity, touching also on the regulation of the cloud market, in order to ensure competition among service providers.

DATA PROTECTION

General Data Protection Regulation (GDPR) (2016)⁶. The GDPR protects personal data of natural persons (independently of their nationality or place of residence) and applies to any organisation processing such data, regardless of location. It also regulates data transfers outside the EU through mechanisms like Standard Contractual Clauses (SCCs) and adequacy decisions. As such, it impacts cloud services in a number of ways, for instance: 1) Cloud providers must ensure personal data security and lawful processing; 2) Organisations using cloud services must sign Data Processing Agreements (DPAs); 3) Use of non-EU cloud providers requires compliance with SCCs or the EU-US Data Privacy Framework.

EU-US Data Privacy Framework (2023)⁷. This framework (DPF) regulates transatlantic data transfers between the EU and the U.S. and it introduces stronger safeguards for U.S.-based cloud providers handling EU data at the same time that it ensures that EU businesses put in place valid transfer mechanisms when using U.S.-based clouds. Partly, this framework was put in place as a reply to the U.S. Cloud Act that allows U.S. law enforcement to request

data from U.S.-based cloud service providers, even if the data is stored outside the U.S. The DPF tries to mitigate the data protection concerns (especially in regards to the GDPR) raised by the U.S. Cloud Act, and introduces specific safeguards designed to limit its perceived overreach.

European Data Act (applicable from 12/09/2025)⁸.

It regulates data access and sharing across cloud platforms. It also aims to reduce vendor lock-in and ensure data portability, introducing rules for switching cloud providers without high costs, adding an additional layer to the Digital Markets Act in order to ensure competition in the cloud services landscape. It also complements the Data Governance Act, that became applicable in September 2023. While the Data Governance Act increases trust in voluntary data-sharing mechanisms, the Data Act provides legal clarity regarding the access to and use of data.

CYBERSECURITY

The Cybersecurity Act (CSA) (2019)⁹. It introduces a harmonised European framework for the EU cybersecurity certification of ICT products, services and processes. The main objective of the CSA is to improve protection against threats to cybersecurity within the EU. The CSA also enables manufacturers and service providers to use one mutually recognised certificate throughout the EU. As part of the CSA, the European cybersecurity agency (ENISA) is working on a European cybersecurity certification scheme for cloud services (EUCS). The scheme will provide increased assurance to businesses, public administrations and citizens that their data are secure wherever they are stored or processed. To that end it introduces standardized security levels for cloud services, and it may include data localization requirements (favouring EU-based datacentres).

Network and Information Security Directive 2 (NIS2) (2023)¹⁰. This legislation applies to general critical digital infrastructure, including cloud computing. It strengthens cybersecurity requirements for cloud service providers, requiring risk management, incident reporting, and compliance audits.

⁵ [EU Digital Strategy](#)

⁶ Regulation (EU) 2016/679, OJ L 119, 4.5.2016, p. 1–88

⁷ Commission Implementing Decision EU 2023/1795, OJ L 231, 20.9.2023, p. 118–229

⁸ Regulation (EU) 2023/2854, OJ L, 2023/2854, 22.12.2023

⁹ Regulation (EU) 2019/881, OJ L 151, 7.6.2019, p. 15–69

¹⁰ Directive (EU) 2022/2555, OJ L 333, 27.12.2022, p. 80–152

The EUIBA Cybersecurity Regulation (2023)¹¹.

This regulation aims to ensure a high common level of cybersecurity in all EU Institutions, Bodies, offices and Agencies (EUIBA). It provides for: 1) the establishment of an internal cybersecurity risk management, governance and control framework for each Union entity; 2) cybersecurity risk management, reporting and information sharing; 3) the creation of an Interinstitutional Cybersecurity Board and the extension of the mandate for the Cybersecurity Service for the Union Institutions, Bodies, Offices and Agencies (CERT-EU).

Even though not directly focused on regulating the cloud computing market, it is worth mentioning here as well the AI Act (2024)¹² as part of the EU legislation that has an impact on cloud technologies. Currently, most cloud service providers offer, as part of their cloud packages, AI-based tools that provide data processing and analysis capabilities to their clients. As such, these applications need to comply with the rules set for AI technology in the AI Act, according to its 4-level risk approach.

Given the highly complex regulatory framework laid out above, the EU plans to compile a set of rules, in the form of an EU Cloud Rulebook and a Guidance on public procurement of data processing services. The Rulebook will provide in a single European framework relevant binding and non-binding rules for cloud service users and providers in Europe. To increase efficiency and quality of public procurement of data processing services in Europe, the Guidance will propose recommendations for implementing consistent national policies complemented by a comprehensive set of essential criteria for data processing services (including cloud-based services) to be considered by public sector bodies during the tendering process.

HOW CAN eu-LISA LEVERAGE ON CLOUD TECHNOLOGIES?

As a result of the abolishment of the internal borders following the Schengen Agreement, the EU put in place a series of compensatory measures to strengthen the external Schengen border. These measures are implemented through a set of inte-

grated large-scale IT systems, that are the result of the evolution of border management at the EU level which, for almost a decade now, has been marked by an acceleration of digitalisation and the adoption of technologies that serve two simultaneous objectives:

1. To enable stronger security and more safety within the Schengen space;

2. To make border crossings to the Schengen area simpler, smoother and faster for travellers, carriers and border guards.

The EU Agency eu-LISA was created in 2012 and mandated with the operational management, development and evolution of, initially, three of these large scale IT systems: the Schengen Information System (SIS), the Visa Information Systems (VIS), and the European Dactyloscopy Database (EURODAC). Since its inception, the Agency has seen a substantial growth of its responsibilities and is currently overseeing a significant expansion of new systems, including¹³: the Entry Exit System (EES), the European Travel Information and Authorisation System (ETIAS), the European Criminal Record Information System for Third Country Nationals (ECRIS-TCN), and their interoperability. The Agency has also taken over other additional projects such as: the e-Justice Communication via Online Data Exchange (eCODEX), the Joint Investigation Teams (JIT) platform, the new e-VISA application platform and its interconnection with VIS, and the new PRÜM II centralised interconnection router. The EES and ETIAS will also have to be made compatible with the Passenger Name Record (PNR) and the Advanced Passenger Information (API). All these new systems necessitate a significant IT capacity upgrade in terms of computational power, data storage, energy, cooling and space.

This recent influx of systems that the Agency has been tasked with developing and managing has resulted in a number of challenges deriving from the physical on-premises limitations that the Agency faces today, and that hinders its ability to expand and accommodate, in a fast and agile way to the new demands.

In this context, cloud computing may be the answer to solving the puzzle for eu-LISA. Always in confor-

¹¹ Regulation (EU, Euratom) 2023/2841, OJ L, 2023/2841, 18.12.2023

¹² Regulation (EU) 2024/1689, OJ L, 2024/1689, 12.7.2024

¹³ For further information about all the following systems and project we refer the reader to [eu-LISA's Single Programming Document 2025-2027 \(SPD\)](#).

mance with the relevant regulations, the Agency could take advantage of cloud technology to:

- Optimise infrastructure utilization and costs by leveraging the elasticity and pay-as-you-go models of cloud platforms.
- Increase operational efficiency through automation and managed services, reducing the burden on staff.
- Improve agility and reduce time-to-market for new systems and updates by utilising cloud-native development and deployment practices.
- Enhance scalability and elasticity to meet changing demands, particularly for non-production environments used in development and testing.
- Reduce its carbon footprint by migrating part of its IT processes to more energy efficient and sustainable datacentres offered by cloud providers compared to the somewhat outdated technology deployed in its on-premises infrastructure.

The cloud could offer some clear benefits to the Agency and, in turn, also improve the quality of service that it provides to Member States. However, such a paradigm shift from fully on-premises operations to a cloud-based approach, would not come without a number of risks. These risks would need to be carefully considered to put in place the necessary preventive measures. The main risks, already mentioned above, include:



Data protection: Safeguarding of data is of paramount importance for the Agency's business. Any potential cloud-based solution would have to guarantee the same level of data

protection currently provided by the Agency through its on-premises service.



Security: The Agency operates under very strict security measures (e.g., security and privacy by design, encryption, access controls, proactive security monitoring, and security inci-

dent response) as requested by the applicable regulatory framework to maintain the trust of stakeholders. Any migration of processes to the cloud should in no case jeopardise the security level currently ensured by eu-LISA.



Sovereignty: eu-LISA operates in a highly sensitive domain and therefore needs to ensure the sovereignty over

its data and applications. This entails that, when considering technological changes in its key processes, the Agency should prevent vendor lock-in situations and favour EU-based solutions, avoiding any type of data transfer outside the Schengen territory.



Compliance: eu-LISA operates under very stringent requirements regarding performance (e.g., short response times for searches), stability of its applications (e.g., aiming for a 99.99% availability for

production platforms) and sustainability of the technologies used, adhering to the largest extent to standardised options.

To maximise the benefits while limiting the risks for eu-LISA, in compliance with the applicable regulations, the Agency has designed a cloud strategy based on a hybrid multi-cloud model¹⁴. This strategy ensures the organisation to maintain control on-premises of its most sensitive assets and processes, while at the same time allowing for agility and flexibility necessary to adapt to the increasing demands of its new systems, avoiding vendor lock-in situations and guaranteeing the stability of services (using multiple cloud providers).

In summary, the hybrid multi-cloud strategy has the advantage for eu-LISA to efficiently manage the growth in the number of large-scale IT systems managed, optimise IT costs and performance, and maintain compliance with EU regulations. It also helps to increase scalability and flexibility regarding IT infrastructure and reduce the time-to-market of new future systems, while maintaining the current levels of security and data protection.

CONCLUSION

In the coming years, how organisations gather, process, secure, store and control access to their data (especially if they are looking to tap new, data-based technologies like Artificial Intelligence and Machine Learning) will have big implications on the quality of the services they provide. That is why organisations are more and more looking to leverage through cloud computing frameworks. At this point, there is a large consensus that the advantages of cloud computing outweigh its limitations. Most organisations today are not considering whether they should migrate to the cloud but what, how and when they should migrate.

The cloud delivers more flexibility and reliability, increased performance and efficiency, and, if pro-

¹⁴ eu-LISA Core Business Systems cloud strategy

perly planned, can help to lower IT costs. It also has the potential to improve innovation, allowing organisations to incorporate AI and ML use-cases into their strategies in a faster and more seamless manner. This can also help to boost productivity, support remote workforces, and improve operational efficiency.

Cloud computing has the potential to transform IT, not necessarily through its impact on an organisation's core business systems, but through making more efficient routine services such as e-mail, web servers, and data storage. Cloud computing can also easily deliver services that are common across the public sector, such as accounting, procurement, and collaboration tools.

It is important to remember that embarking on a cloud journey is not necessarily an all-or-nothing scenario. Adopting a hybrid approach can help extend the capacity and capabilities of existing infrastructure while still operating in the environment that works best for the overall business.

However, despite all their benefits, cloud technologies also bring some risks that require the necessary protection measures. Before selecting a cloud model and service, any institution should carefully analyse factors such as: security, data governance and data protection, performance, regulatory compliance, or resiliency.

Independently of the cloud model selected, nowadays, it is essential for any organisation to put in place a strong cloud migration strategy that includes:

Training: Staff members in policymaking positions need to learn about cloud computing and the potential it holds.

Organisational assessment: It is critical to conduct an examination of the organization's real and anticipated IT utilisation and how cloud-based storage, applications, and processing power might replace or supplement present IT capacity.

Cloud-readiness assessment: It is important to determine where cloud can (and cannot) be used as part of the organization's overall IT portfolio.

Cloud pilots: One or several small-scale pilot projects can be used to test how cloud works for an organisation, with the existing technology and staff.

Cloud rollout strategy: Integrate cloud offerings as part of the organisation's overall IT strategy and work to gain buy-in to the change effort throughout the organisation.

Continuous cloud improvement: Eventually, cloud resources will become part of the everyday work of the organisation, which will necessitate making decisions as to when and how to best make use of cloud storage and applications.

A solid approach to cloud monitoring and management: By setting up a systematic approach to the monitoring and management of utilisation of cloud resources, organisations will be able to avoid overprovisioning and inefficient utilisation of cloud resources, and the associated costs.

TECHNOLOGY BRIEF

eu-LISA 

Technology Brief completed in June 2025

Neither eu-LISA nor any person acting on behalf of eu-LISA is responsible for the use that might be made of the following information.

Luxembourg: Publications Office of the European Union, 2025

ISBN 978-92-95237-02-5

ISSN 2812-0795 doi:10.2857/4721859

Catalogue number: EL-01-25-002-EN-N

© eu-LISA, 2025

Reproduction is authorised provided the source is acknowledged.

For any use or reproduction of elements that are not owned by eu-LISA, permission may need to be sought directly from the respective rightholders. eu-LISA does not own the copyright in relation to the following elements: