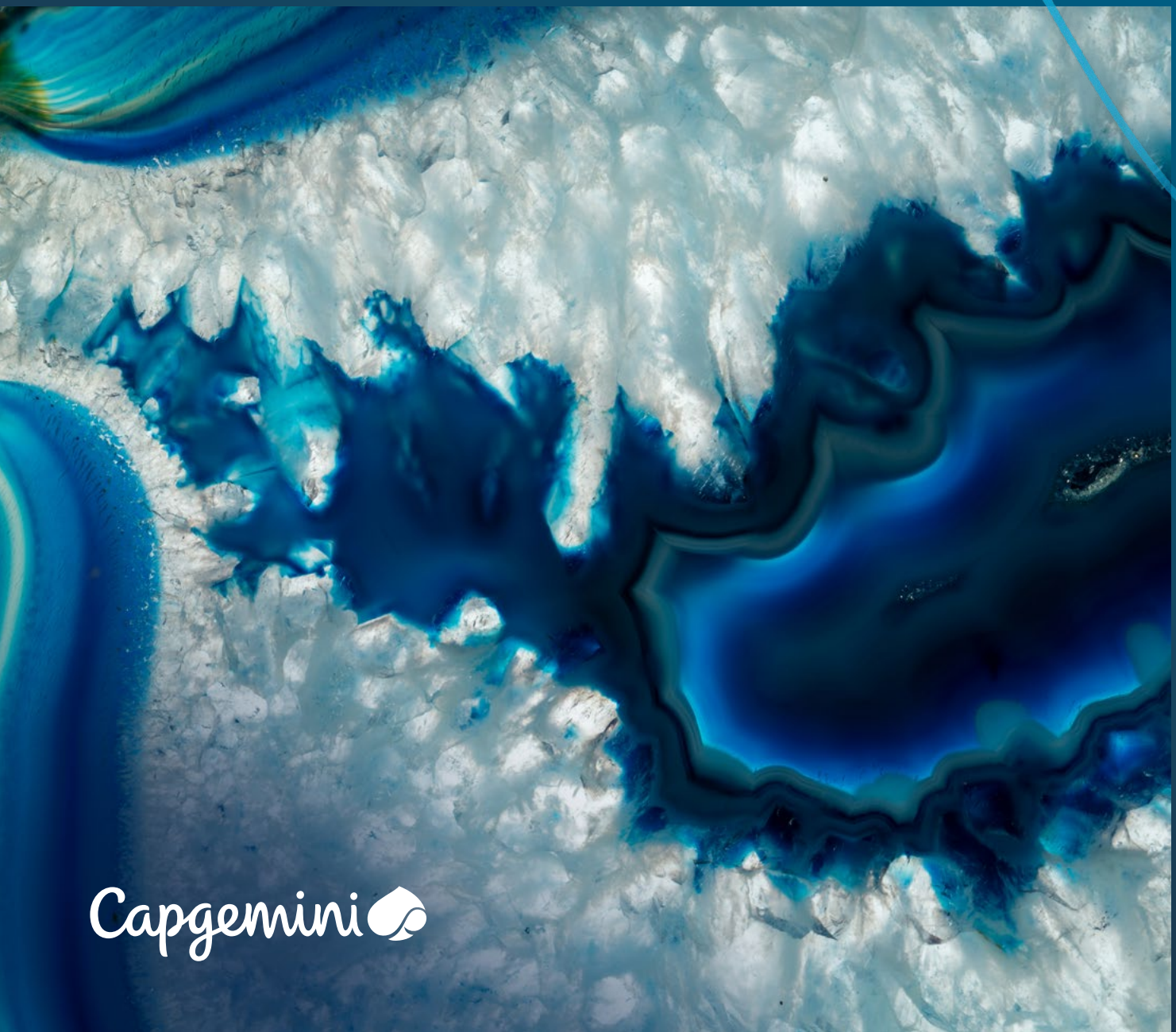
Trusted **cloud**

Combining performance,
innovation and sovereignty



Capgemini

Adding **TRUST** to Sovereign Cloud

Digital transformation in Europe is at a crossroads. Governments and businesses recognize a need for sovereignty. Will that lead to a future where they are masters of their own digital domain?

Cloud providers have launched many sovereign cloud initiatives in the last two years. These choices can make organizations more independent, but the right definition and criteria of sovereignty must be found to implement long-term digitization in industry and government.

It is therefore also a question of trust. Which provider and which technology do we trust to make long-term transformations and investments in key areas? Trusted cloud is therefore a term that we at Capgemini use to describe precisely this target environment.

A trusted cloud is not only relevant for the public sector, but also increasingly for critical industries and regulated markets. This paper summarizes the most important points in this discussion and hopefully provides valuable starting points for a discussion on the use of a trusted cloud.

Choosing no longer means giving something up

The cloud is a complex equation with multiple variables. Migration to the cloud serves two purposes that until now might have seemed mutually exclusive: On the one hand, it offers the possibility of innovating in data processing to improve performance and customer experience; on the other hand, it optimizes operational costs, creating an essential balance for companies.

In a world where challenges are multiplying and intensifying, sovereignty is emerging as one of the best shields against risks of various kinds, notably legal, economic and reputational.

The trusted cloud is becoming a relevant alternative or complement to the public and private clouds that dominate the market today, guaranteeing enhanced security and compliance with national and European data protection standards. In fact, this is the first time that it has been regulations (rather than business needs or technology) that have driven such an evolution.

The trusted cloud provides companies with a balance between the need to protect their sensitive information, the performance of their ecosystem and their ability to innovate, while guarding against dependence on non-European cloud providers, who today dominate the market.

The aim of this guide is to define the concept of the trusted cloud, to explore its opportunities and challenges, its benefits and its costs, and to stimulate global thinking on this fast-developing solution and its integration into a multi-cloud approach.

We hope you will find it an enriching read.

Stefan Zosel
VP Sovereign Cloud Public Sector
Capgemini

Pierre Albert
Enterprise Architect
Capgemini

Ambroise Lelievre
Business Technology Director
Capgemini Invent

Sovereignty is acquired and preserved

Nearly nine out of ten organizations see the topic of sovereign cloud gaining in importance in the future and 52% of them are preparing to include sovereignty in their cloud strategy according to a study by the Capgemini Research Institute[1].

Covid-19, conflict in Ukraine, tensions on the global energy, utilities and raw materials market... In Europe, sovereignty has become a major political, geostrategic and economic issue. If the word is on everyone's lips, what is its exact definition? Sovereignty is understood as the nature of a state that is not subject to any other state. We want independence. However, the digital market is dominated by a handful of American companies.

Thus, the overwhelming majority of cloud spending in Europe goes to Amazon, Google or Microsoft. At the same time, cloud usage (IaaS, PaaS, including private cloud) and massive data growth are progressing at high speed. The equation to be solved is then posed in the following terms: How to enable the innovation brought by cloud technologies while controlling the risks?

The three axes of digital sovereignty:

Digital sovereignty is defined as the ability of countries, organizations and individuals to determine their own digital future.

This has a triple impact on:

Technology

in particular reversibility,

Data

geographic location of servers,

Operations

who carries them out, in what country and with what security level?

[1] *The Journey to Cloud Sovereignty,* Capgemini Research Institute, June 2022

Trusted cloud, a label and guarantees

To respond to the many operational, economic, legal, reputational and cybersecurity risks, governments and security authorities are formulating clearer definitions of their national requirements.

Vendors who meet these requirements will be entitled to use the Trusted Cloud label. For them, this involves running cloud services from national territory, through an entity governed by national law, in strict compliance with national laws and standards. The framework also provides protection against legal risks related to the application of extraterritorial laws (in particular the US FISA and Cloud Act regulations). A great example of that is the French SecNumCloud 3.2[2] which defines a trusted cloud for France.

In a *multicloud strategy*, the trusted cloud completes the sovereignty continuum between two extremes: The public cloud and the private cloud. The first encourages innovation but offers no protection against extraterritorial laws if operated by one of the major cloud service providers (hyperscalers). The second is often sovereign by design, but is quickly restricted from the point of view of innovation by a limited range of services. To overcome this dilemma, the trusted cloud allows American companies to license their technology to French companies.

Trusted cloud: how to get started?

The first step in transforming to a trusted cloud is to *identify the risks to be covered*. This analysis cannot be done macroscopically: it involves going down to the level of data clusters and applications.

Once this inventory has been established, a trusted cloud strategy can be defined. It makes it possible to determine which data and which processing operations are intended to remain on premise; which of those are candidates for a trusted cloud and, finally, which can be safely moved to a public cloud.

This strategy is then translated into a move to cloud project, which requires specific points of attention. For example, the topic of data encryption and associated key management deserves specific treatment due to the sensitivity of the data. For some organizations, the collaborative side (messaging and collaborative tools) can represent a significant part of the *migration to a trusted cloud*.

While migrating the right data and processing to a trusted cloud is a first challenge, maintaining the acquired digital sovereignty over time is the second objective to keep in mind from the start of the journey.

[2] To respond to the many operational, economic, legal, reputational and cybersecurity risks, ANSSI has established demanding specifications, called SecNumCloud 3.2.

A long-term approach to change management

Sovereignty is only lost if it's not used! Once the migration to a trusted cloud has been completed, it is also important to design and implement the best practices for day-to-day operations (run phase) that will ensure digital sovereignty over the long term.

There are four disciplines to be covered in this area:

1. **Changing architectural practices:** which establishes sovereignty by design.

2. **Trusted operations or "SovOps":** how do we operate processing and manage data hosted in a trusted cloud? With what staff?

3. **Cybersecurity in the trusted cloud:** to be distinguished from the cybersecurity of the trusted cloud itself provided by the provider. How can best practices be tightened to take account of the criticality of data and processing?

4. **Financial and environmental impact control:** How can we ensure that the usage costs and environmental footprint of the trusted cloud are kept under control?

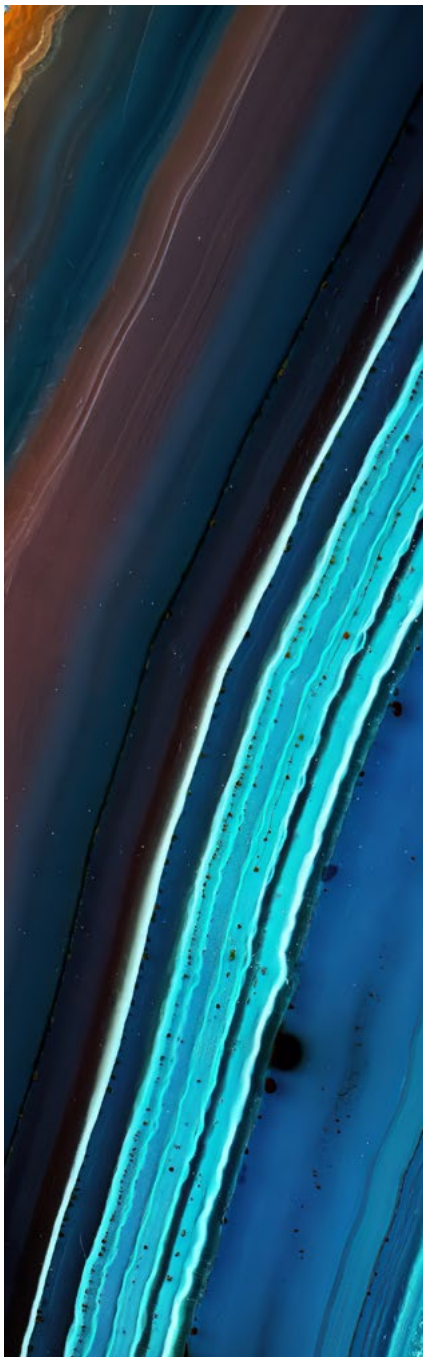
Five risks to anticipate

In order to benefit from the performance and innovation advantages of the cloud, organizations need to gain a thorough understanding of the risks associated with using the cloud in a changing economic and regulatory context.

1. Legal risks

The cloud ecosystem is evolving in a complex regulatory and legal landscape. States have been legislating for several decades on the processing and hosting of personal and industrial data. Administrations and businesses are then engaged in a normative battle which requires them to reconcile sovereignty and innovation. In this sense, legal risks are structured around two major issues linked to data:

- **Uncontrolled data transfers outside national jurisdiction.** For example, two agreements have successively framed these transfers between the European Union and the United States to establish principles for privacy protection: Safe Harbor and Privacy Shield. Both were invalidated by the Court of Justice of the European Union (CJEU)[3] (Schrems I & Schrems II rulings) because they were deemed non-compliant with the European vision of the protection of personal data (and in particular the GDPR[4]). In March 2022, the European Commission and the United States agreed on an agreement in principle "on a new transatlantic framework for the protection of personal data"[5] in order to provide a response to the legal uncertainty left by these invalidations. In this vein, the executive decree signed by Joe Biden on October 7, 2022 should be followed by validation by the European Commission in the coming months.[6]
- **Capture of data by a foreign entity,** through the use of an extraterritorial tool by a State. Extraterritoriality can be defined as the exercise of legislative authority beyond its territory; in our context, this means the ability of a "non-European State to access all or part of the data and processing hosted by a provider"[7]. This is what is permitted, under certain strict conditions, by the American law Cloud Act (Clarifying Lawful Overseas Use of Data Act). To another extent, the amendments to Section 702 of the FISA (Foreign Intelligence Surveillance Act) – also targeted by the Schrems II ruling in 2020 – constitute a risk of interference with European data.



[3] Court of Justice of the European Union
[4] General Data Protection Regulation
[5] *Joint Statement by the European Commission and the United States on the Transatlantic Data Protection Framework, 25 March 2022*
[6] *FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework*
[7] *Cyber Threat Overview 2021, ANSSI*

2. Operational risks

This refers to all the risks associated with restricting access to cloud services. Due to their strategic and/or governmental nature, some organizations cannot tolerate any incidents or failures, as these could have "a significant disruptive effect on the provision"[8] of their strategic activities (particularly sectors of vital importance such as energy, industry or health).

Reliance on foreign technology or cloud services significantly increases these risks, particularly in the event of geopolitical tensions and crises. These short-term factors have the effect of accelerating the thinking of States and governments on this subject. For example, war in Ukraine has accelerated the thinking of European states on the subject of "the resilience of telecoms infrastructures and the protection of European cyberspace".[9] Companies and administrations should soon be able to include the outcomes of these discussions in order to better understand these uncertainties.

3. Security risks

Where the cloud is concerned, the notion of sovereignty is based on the ability to counter different levels of threats: activist, cybercriminal, and state-sponsored. Risk prevention is partly the responsibility of service providers but also of user organizations.

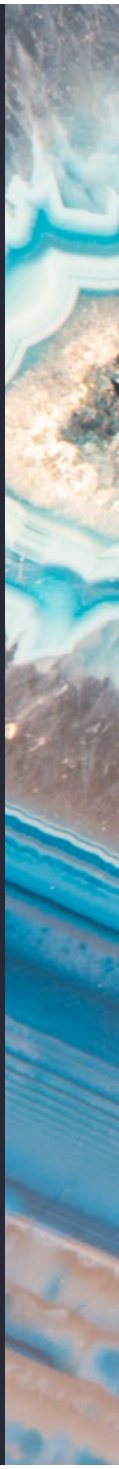
Cyber threats: A sharing of responsibilities between suppliers and users

Cloud Security:

Is the responsibility of the cloud provider (Cloud Service Provider or CSP). Certifications exist to guarantee this aspect, such as the SecNumCloud qualification in France, C5 in Germany and EUCS at a European level. This category also includes the physical risks of disruption linked to the supply chain of services and infrastructure components, exposing organizations to multiple security breaches (not to mention the operational instability induced by dependence on foreign suppliers). The lack of control of physical equipment and servers must also be considered, in order to limit the risk of exposure to espionage activities. Cloud security, which refers to the mechanisms adopted by user organizations to secure the data hosted and the processing that is performed in the cloud. These mechanisms can either be entirely the responsibility of the customer (data encryption) or be based on a shared responsibility model (the supplier provides security services that the customer is responsible for configuring and operating).

Security in the cloud:

Which refers to the mechanisms adopted by user organizations to secure the data hosted and the processing that is performed in the cloud. These mechanisms can either be entirely the responsibility of the customer (data encryption) or be based on a shared responsibility model (the supplier provides security services that the customer is responsible for configuring and operating).



[8] *NIS Directive*
[9] *Cybersecurity and telecom network resilience: EU strategy hastened by the Ukraine war*

4. Economic risks

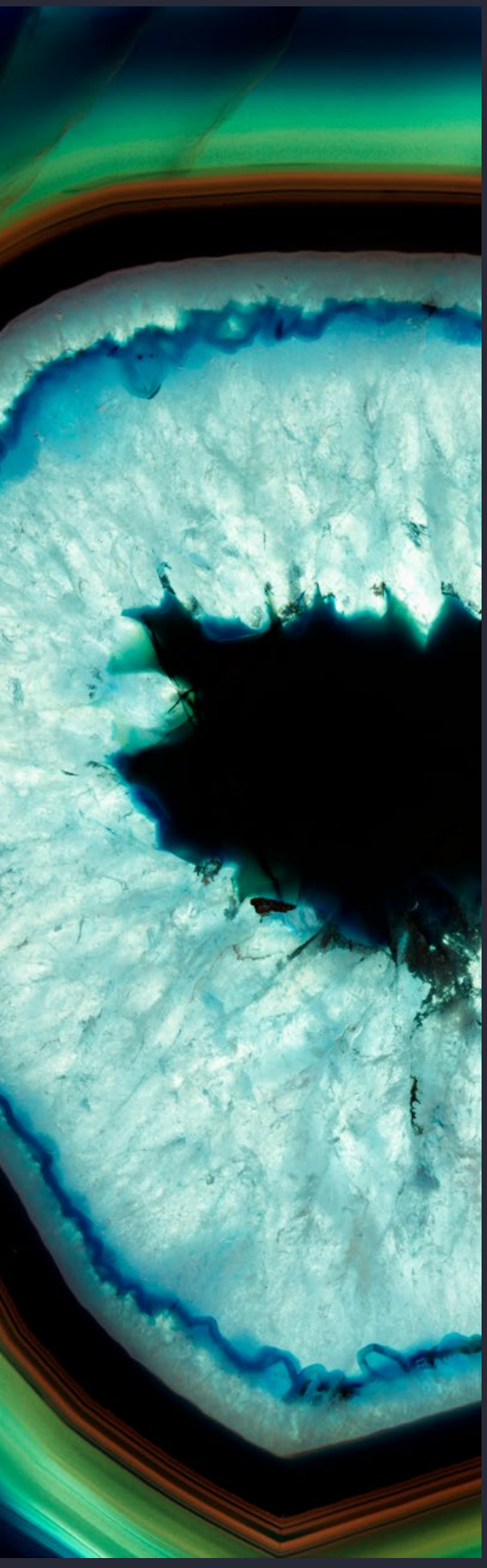
Industrial espionage[10] aimed at acquiring strategic data also poses significant economic risks to organizations[11]. At the same time, the lack of transparency of certain cloud services is raising concerns about value capture in a market dominated by mainly American players. Some industries and state administrations are struggling to develop innovative use cases while ensuring the protection and confidentiality of their "sensitive data", due to the lack of trusted solutions – which impacts their level of competitiveness.

The lack of reversibility and portability is also proving to be an obstacle to exploiting the value of this data via cloud services. Finally, economic risks are also linked to the risk of legal and regulatory non-compliance, for example a situation of non-compliance with the GDPR can lead to financial penalties of up to 4% of a company's annual global turnover.[12]

5. Reputational risks

These risks concern any potential reputational damage caused by the interruption of a service, whether accidental (natural disaster) or intentional (cyberattack). They are again exacerbated by technological and economic dependence on foreign actors. These risks are also heightened in Europe, where citizens are sensitive to the management of their data and the protection of their privacy.

[10] Ibid
[11] *Main incidents in the EU and worldwide – ENISA, 2020*
[12] *CNIL*



Trusted Cloud: a subtle balance between security and innovation

Organisations should therefore be aware of all compliance requirements imposed by their country as well as those applicable to their sector of activity[13]. Cloud compliance is defined as compliance with processing and hosting standards arising from local laws and regulations (for example the French military programming law[14]), European (GDPR) and sector-specific laws and regulations (such as the specific case of health data). It is also imperative to identify and understand risks related to regulations with extraterritorial scope (for example, if the data is hosted within a cloud owned by a foreign company). Given the changing nature of regulations, monitoring must be established in order to maintain compliance over time. This phase must be supported by legal expertise.

Then the next step is to define a perimeter eligible for migration to a trusted cloud. This signposting step must be built jointly with several stakeholders in the organization (including business & IT teams) — including CDOs (Chief Data Officers) and DPOs (Data Protection Officers) — and must be fully integrated into a broader hybrid and multicloud strategy.

Data classification must take into account two main elements: The aforementioned risks and the level of sensitivity of the data. This reflection must be focused on business use cases.

At the end of this consideration, the choice of the most suitable cloud offers can be made, in line with security constraints (access to data, encryption techniques, key management), sovereignty (location restrictions, technology used, operations management, resilience), and the ambition to innovate (service catalog, partner ecosystem, etc.). The transformation to the trusted cloud must also include a trade-off between the constraints of a multi-cloud or hybrid architecture, including interoperability, interconnection, end-to-end compliance and associated costs[15].

The trusted cloud thus makes it possible to mitigate these various interconnected risks, while allowing companies and administrations to benefit from the state of the art technology involving innovation, velocity and performance.

[13] *The Journey To Cloud Sovereignty* – Assessing cloud potential to drive transformation and build trust, Capgemini Research Institute, 2022

[14] Military Planning Act, 2013

[15] *The Journey To Cloud Sovereignty* – Assessing cloud potential to drive transformation and build trust, Capgemini Research Institute, 2022

Cloud Trust: What are its **benefits**? And at what cost?

The Trusted cloud offers an alternative to public cloud services for organizations facing regulatory and/or sovereignty constraints. However, they need to successfully manage its costs to maximize its value.

The trusted cloud offers significant advantages:

- Security and protection against extraterritorial laws. Thanks to its sovereign nature, it is impervious to non-European laws (American Cloud Act, etc.).
- Enhanced cloud protection with robust infrastructures and effective, state-of-the-art defense measures against external threats;
- Optimal security in the cloud. It integrates advanced access control, encryption and monitoring mechanisms, allowing companies to effectively protect the integrity and confidentiality of their data;
- Optimal security in natively available security resources and processes – unlike traditional public clouds. This makes it possible to limit the investment and maintenance of third-party security solutions.

Additional costs

However, the benefits come at a cost. With trusted cloud, customers can expect to pay 10-20% more than with traditional public cloud offerings, due to enhanced security and compliance measures.

In addition, implementing a trusted operating model generates additional costs: training future user teams, but also deploying specific processes to guarantee security in the cloud.

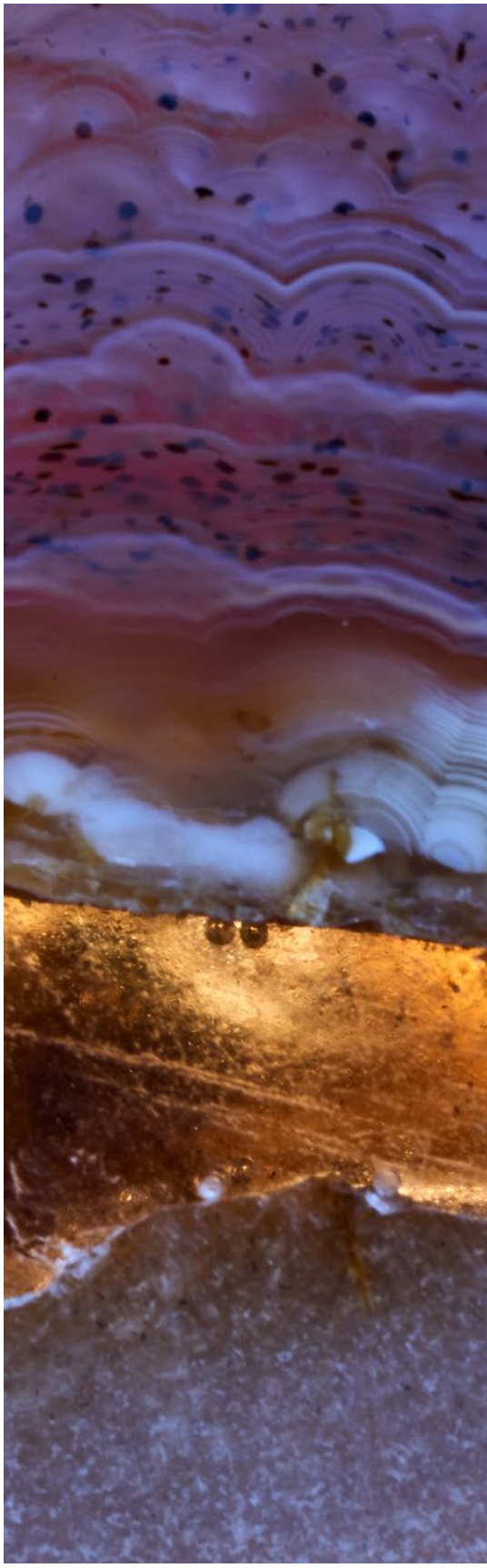
Finally, integration and interoperability with the information systems of entities and subsidiaries located outside the European Union may also entail additional costs. Companies must then deploy means of interconnection between their cloud platforms.

A cost-benefit trade-off in favor of the trusted cloud

Despite these additional costs, the economic equation of the Trusted Cloud can prove favorable for organizations wishing to combine sovereignty, security, agility and innovation.

In most cases, this involves switching from an existing, already optimized system. Estimating the costs associated with sovereignty must take into account the state of existing information systems, which are often already optimized or even amortized, whether or not they are hosted in the public cloud.

Careful thought is needed to determine the strategy best suited to the company, whether this involves adopting a multicloud model, switching entirely to the trusted cloud, or opting for a hybrid approach by keeping some systems on site (on-premise).



Maximizing the value of your trusted cloud

To get the most out of the trusted cloud, while keeping costs down, organizations need to start thinking about this issue at the very beginning of the project, and continue to pursue a virtuous FinOps approach throughout.

Migration to a trusted cloud offers organizations that have already carried out an initial cloud migration the opportunity to start from a clean slate and return to the state of the art. To maximize the value of this transition, several elements must be considered:

- **Manage** business case studies with the utmost precision and diligence, in order to ensure the best possible results.
- **Design** efficient landing zones to facilitate the migration of applications and optimize their management once deployed in the trusted cloud.
- **Anticipate** start-up latency, particularly in the case of SaaS solutions that will not be immediately available in a “trusted” version.
- **Automate** processes to the extent possible (particularly around provisioning) to reduce costs and increase the agility of the organization.
- **Use** hybrid architectures to leverage the best features of each environment and ensure a smooth transition.
- **Anticipate** contractual negotiations: there is unlikely to be any overlap between the master agreements of the major cloud providers (hyperscalers) and their “trusted” equivalents.

Continuous optimization with FinOps

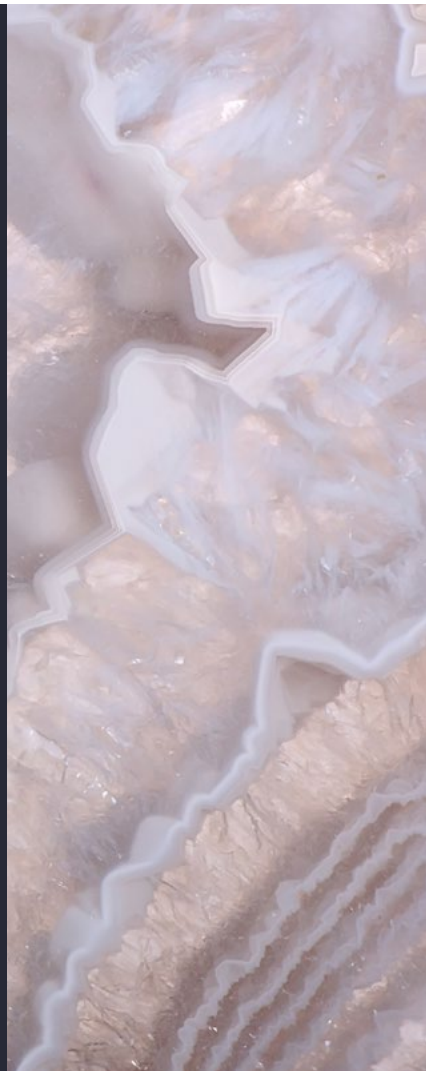
The trusted cloud certainly offers major advantages in terms of sovereignty and security of services and data, but without optimization, it can generate additional costs. To maximize the value, a proactive approach is necessary from the start of projects, with the involvement of all stakeholders including business managers, who are responsible for the expenses incurred in their areas. Teams must be trained in these best practices for efficient use of resources and services.

It is also essential to apply strict policies regarding the selection of security levels, in the interests of cost control and compliance.

Finally, FinOps principles need to be systematized. This involves setting up dashboards and alerts to closely monitor changes in costs and performance. Automating the application of FinOps principles (policy as code) makes particular sense here.

FinOps: obstacles yet to be overcome

Not all FinOps tools and services (especially SaaS) will be immediately available on trusted clouds. Alternatives will need to be analyzed: Use the services offered natively by suppliers (similar to the public cloud), deploy other software packages or carry out internal developments.



The pillars of trusted cloud migration

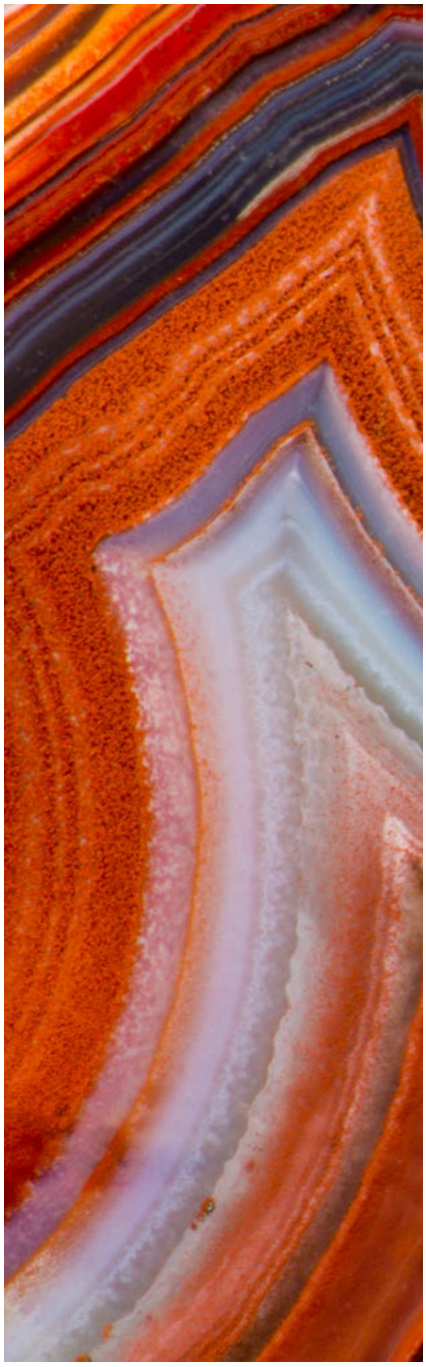
There are many challenges for organizations: business innovation, operational and organizational efficiency, IT resilience and cybersecurity, not to mention sovereignty and sustainability. Multiple variables are added to an already complex equation that few players seem to have fully mastered.

Digital maturity

The maturity of the companies and public institutions concerned is highly heterogeneous. Some are already comfortably installed on public clouds (with cloud-first or cloud-native strategies), while others are complementing their on-premise IS or private cloud with public clouds, but only for certain specific uses (hybrid clouds, interoperability). A third category of companies has chosen not to interface with any of the American giants and still operates entirely on their private cloud/on-site in complete autonomy.

Diagnosis of existing situation

Every migration project begins with a diagnostic phase, aimed at taking detailed stock of the existing applications, technologies and organization. It will first be necessary to assess the risks and also to identify, qualify and classify the data, processing and applications in order to determine their destination (on site, trusted cloud, public cloud).



What data to migrate?

The scope of data subject to migration to a trusted cloud depends on a combination of parameters: their sensitivity (from very secret to unprotected), their types (strategic business data, economic data, personal data, and health data), the depth and ambitions of the migration (IaaS, PaaS or SaaS). This crucial exercise, which contributes to the diagnosis of the existing situation, will thus make it possible to identify candidate data sets for migration to a trusted cloud.

Which partners to choose?

Today, there are just under a dozen trusted cloud offerings in Europe, with catalogs of varying depth (from IaaS, PaaS to managed SaaS solutions). The majority of these offers naturally rely on Azure, Google, AWS, or national players like BLEU/Delos, OVHCloud, StackIT, IONOS and many more. However, they still seem rather limited in scope to meet end-to-end business processes which could frustrate certain migration ambitions for the most appealing players, and therefore reinforce the use of a multicloud strategy in the short term.

In a market that is evolving as quickly as that of trusted digital technology, organizations are having difficulty realizing their projects. How to establish the right migration strategy and associated roadmap when a more suitable offer could come out at any time? That's why it's essential to keep an eye on the competition, and to be able to quickly pivot your strategy towards the most suitable solution.

When automation strengthens digital sovereignty

Thanks to automation, companies can meet security and digital sovereignty challenges with local or European personnel, at acceptable costs, while adopting a sustainable approach.

Many businesses want to benefit from reliable and secure IT infrastructures, while also supporting the local economy. Automation and infrastructure management tools make it possible to relocate activities within local territory, with implementation costs that are competitive with current offshore solutions. This approach enables us to meet the challenges of sovereignty by locating high value-added activities locally or nationally, increasing the speed of delivery, making infrastructure management actions more reliable, upgrading systems and reducing infrastructure management costs.

Hyperautomation aims to automate end-to-end IT infrastructure management processes and functions, without human intervention:

- Observability of the information system;
- service management (management of incidents, problems, changes, etc.),
- AIOps (intelligent operations such as correlations, root cause or impact analyses, business service operation forecasts, intelligent task processing services, etc.)
- service reporting and dashboards. All these elements are orchestrated and interconnected by modern and recent automation tools as well as other enterprise exchange buses.
- This approach improves speed (processing time), reliability (reduction of errors) and efficiency (accuracy of operations).

Cybersecurity, a shared responsibility

Businesses and institutions choose the trusted cloud to securely handle sensitive data. Services labeled "trusted cloud" provide a number of guarantees for securing the environment, in addition to the measures taken by customers (applications, data, processes).

Identity and access management

Identity and Access Management (IAM) is the cornerstone of cloud security. Managing identity, authentication and permissions, it ensures that users — human or machine — can only access the data and applications that are authorized to them.

Essential and omnipresent, IAM not only determines the level of security in the cloud, but also greatly facilitates the fluidity of exchanges, experiences and projects. IAM is also the cornerstone of the zero-trust model. IAM is also the keystone of the zero trust model. Based on a systematic verification of identities and rights before each action, and not just when accessing the system, this approach requires highly sophisticated, largely automated rights management, granting each user only those authorizations that are strictly necessary. Therefore, the zero trust model can be considered as a global approach to protect the cloud environment and its components (identity, network, data, etc.). In addition, implementing a trusted operating model generates additional costs: Train future user teams, but also deploy specific processes to guarantee security in the cloud.

Defense in depth

In addition to access, each layer of the infrastructure must be specifically secured. This is the principle of Defense in Depth (DiD), a cybersecurity doctrine which consists of establishing several lines of defense (at the hardware, software, network level, etc.) to protect information.

In the context of the trusted cloud, this layered approach must be coordinated with the measures taken by the cloud provider to physically protect its systems. This is why it is often relevant to rely on the security tools and services it offers (firewalls, antivirus, etc.).

Often of good quality, these solutions have the advantage of being natively integrated into the platform, which facilitates their implementation. Finally, it should be emphasized here that the various safety measures still depend on the prudence of users (within the limits of the layers for which they are responsible). Their

implementation must therefore be accompanied by a strengthening of practices in the context of the cloud: Destruction of unnecessary resources and data, automation of updates, security by design, DevSecOps (Development, Security, Operations)…

Encryption: protecting sensitive data

To effectively protect your data, encryption remains fundamental. Its implementation in a trusted cloud, and therefore on the most sensitive data, does however present a few specificities. It is therefore necessary to ensure that the data will remain permanently in the controlled environment of the trusted cloud and will not be exfiltrated, at the time of their processing, to a platform which would not benefit from the same legal protections.

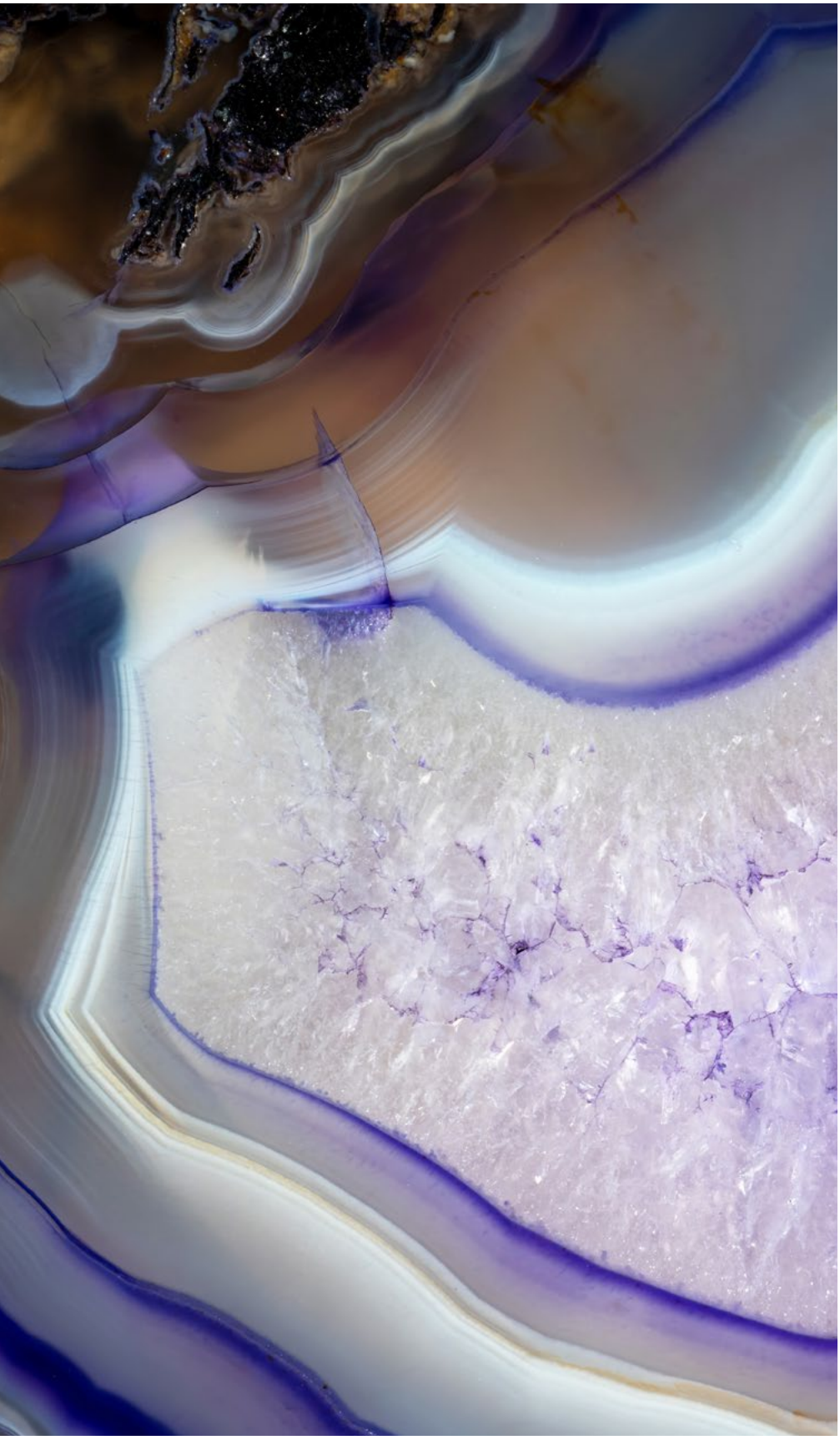
To monitor data leaks and transfers from one environment to another, it is essential to implement specific tools, such as CASB-like solutions that interface with cloud services and control data flows throughout their life cycle.

The choice of third-party tools for manipulating data must be given extra care. In particular, it must be ensured that no operation is carried out outside an environment labeled “trusted cloud”, as this is what is at stake: data can circulate between systems, but it must never leave this protective framework, even for a short time. And it is essential to make all teams aware of this crucial requirement.

One final point of caution when it comes to data: ensure that encryption keys are not stored in the same place as the data, so that they cannot be accessed simultaneously. Hardware Security Modules (HSMs) can be used for this purpose. ensure that encryption keys are not stored in the same location as data so that they cannot be accessed simultaneously. For this purpose, dedicated hardware (Hardware Security Module, HSM) can be used.

Assume Breach

In an environment as complex and ever-changing as the cloud, even if it is a trusted one, and in the face of highly skilled, equipped and determined attackers, absolute security does not exist. This is the principle of the Assume Breach posture, which invites us to be realistic and pragmatic. Since a security incident will always occur, we need to be prepared to detect and warn of it as early as possible, to react quickly and appropriately to limit its consequences, to repair any damage and, finally, to learn from it. All this requires the implementation of appropriate tools, organization and processes, which full-scale exercises will allow to test, validate and optimize.



Secure Data Migration

Just like moving house, which sometimes leads us to leave doors wide open and objects unattended, migration operations generate significant risks. Whether the starting or ending point is a trusted cloud can only heighten these risks by arousing malicious interests. Therefore, even if the operations are similar to those of a migration to the standard cloud, it is necessary to proceed with increased rigor, relying in particular on encryption. You should also not forget to erase the data from the original platform.

All these solutions and best practices help to double the guarantees provided by the trusted cloud with a complete and reinforced security system. However, their implementation-as well as the choice of a trusted cloud-requires an upstream assessment of the risks involved, i.e. the relationship between the seriousness and probability of the threats. This analysis makes it possible to determine the right level of protection to implement and the priority of actions to be taken, taking into account all constraints and requirements (regulatory, budgetary, operational, etc.).

Risk Management in a Multicloud Strategy

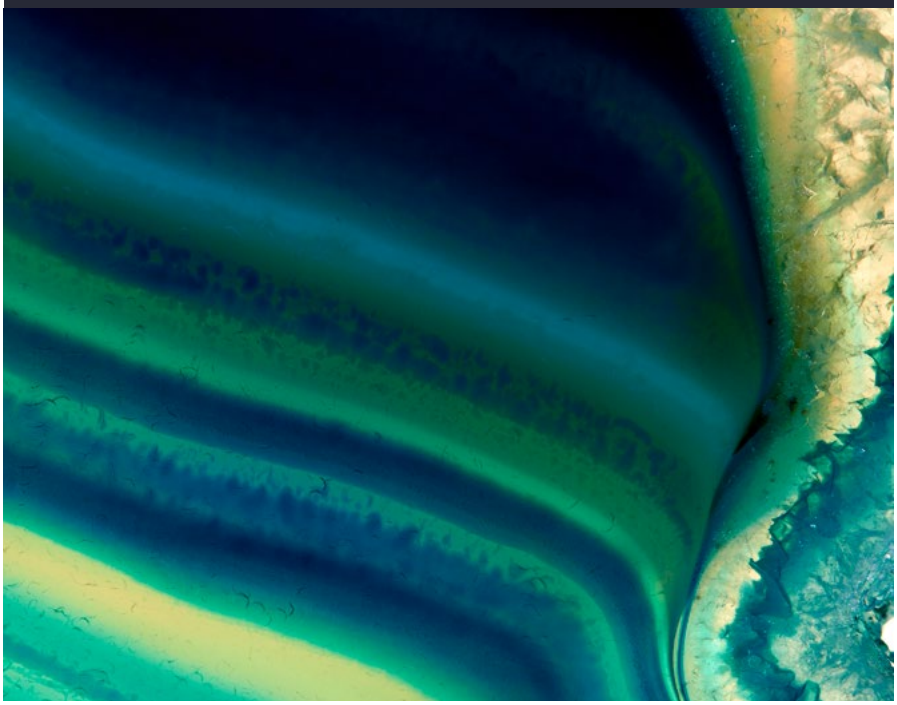
The issue of digital sovereignty is not new, it has always existed when formulating cloud strategies. The major change is the emergence of new offerings.

In recent years, the digital transformation of business activities has been a binary choice: Either they could be moved to a public cloud, or they had to remain in an on-premises infrastructure, ideally a private cloud built and managed under the strict control of the company. The trade-off was therefore between a rich catalogue of external services under the direct control of a third party, or an internally controlled infrastructure with a more limited set of services. While this principle of designing cloud strategies has not fundamentally changed, the possibilities offered are now more extensive and nuanced, allowing for more sophisticated strategies.

Alongside public and private clouds, the arrival of the trusted cloud offers a 3rd option. It should be noted that the service catalogs of trusted cloud providers tend to be extensive, with services at different stages of maturity and sometimes specialized, making the spectrum of possibilities even wider.

Sovereignty: the stage of maturity for organizations

From a risk management perspective, companies are becoming more mature in dealing with different types of risks: Economic, competitive, geopolitical, regulatory, reputational, to name a few. This new advancement facilitates the analysis of application domains, even individual applications and data portfolios. This increased granularity provides a more precise vision of what the notion of sovereignty concretely means for each organization.



Dynamic multicloud strategies

Although the notion of sovereignty seems immutable, its practical implementation in the cloud sector is fluid, due to multiple parameters:

- **The competitive landscape** of many industries is changing very rapidly, requiring continuous innovation in use cases and data usage.
- **Cloud providers' service catalogs** are growing at a dizzying speed, both for public and private clouds.
- **The regulatory landscape** is constantly evolving – at national and European level.
- **Multiple providers** of innovative trusted cloud services exist or are being announced in a space that is rapidly becoming rich with options.
- **Volatility related to geopolitics** and pandemics is disrupting supply chains, including those of cloud providers. This is not without impact on the balance of strategy – energy costs and disruptions in semiconductor supply chains are part of the equation.

Naturally, the context of each organization has its own characteristics. This requires continuous attention from multidisciplinary teams (cybersecurity experts, business, IT and IT architects) to maintain the balance between control and innovation.

In the specific case of multicloud strategies, almost all projects will be subject to the forces in motion:

- **Projects to adopt innovative technologies** offered by cloud providers, such as AI, big data or low code/no code (these development platforms and tools that allow business users to directly design and develop their applications without needing to code);
- **Existing and future business initiatives** subject to data privacy or residency regulations that evolve over time;
- **The end dates of existing outsourcing contracts,** whether they are IT management or hosting contracts;
- **FinOps approaches**, especially when they involve the use of reserved instances over long periods of time.

The key: anticipation

Most of these issues, including the most difficult ones (such as the evolution of regulations around the sovereign or trusted cloud at a national and an EU level) are already in the hands of management. To make their multicloud strategy a success, they need to assign the right priorities, mobilize the right multidisciplinary resources while accessing the right information, all in the strategic tempo of their business imperatives.

Born at the very end of the 1990s, **the cloud is now experiencing a surge in growt**h, with investments achieving record levels year after year. Added to this is a changing regulatory context, relating to security but also to the requirements now placed on companies in terms of s**ocial and environmental responsibility.**

The trusted cloud carries a key promise: It will soon enable companies to **take advantage of the latest innovations**, such as generative AI, within the framework of a security ecosystem, with the certainty of retaining control over their data.

The challenge for companies will be to adapt to this changing ecosystem, seize opportunities and embrace the constraints linked to new standards. To achieve this, they can count on the support of their technological partners. **This is essential backing, given that the cloud is defined as a complex equation, with multiple variables and in perpetual evolutio**n.

Contributors

Pierre Albert
Enterprise Architect
Capgemini

Serge Baccou
Head of South and Central Europe Azure Cloud COE
Capgemini Invent

Skander Guetari
Expert in Infrastructure Transformation Services
Capgemini

Thomas Sarrazin
FinOps Offer Leader
Capgemini

Lucas Lauret
Cloud Services Manager
Capgemini Invent

Ambroise Lelievre
Director of Business Technology
Capgemini Invent

Abdembi Miraoui
Co-Head of Service Line "Cloud, Endpoint & Infrastructure Security"
Capgemini

Stefan Zosel
VP Sovereign Cloud Public Sector
Capgemini

Camille Sebire
Sovereign Cloud / Trusted Cloud Offer Consultant
Capgemini Invent

Benoit Thibaut
Group Industrialization Design Authority Leader
Capgemini

Thomas Heron
Enterprise Architect
Capgemini

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided every day by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of nearly 350,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering, and platforms. The Group reported in 2022 global revenues of €22 billion.

Get the Future You Want | www.capgemini.com