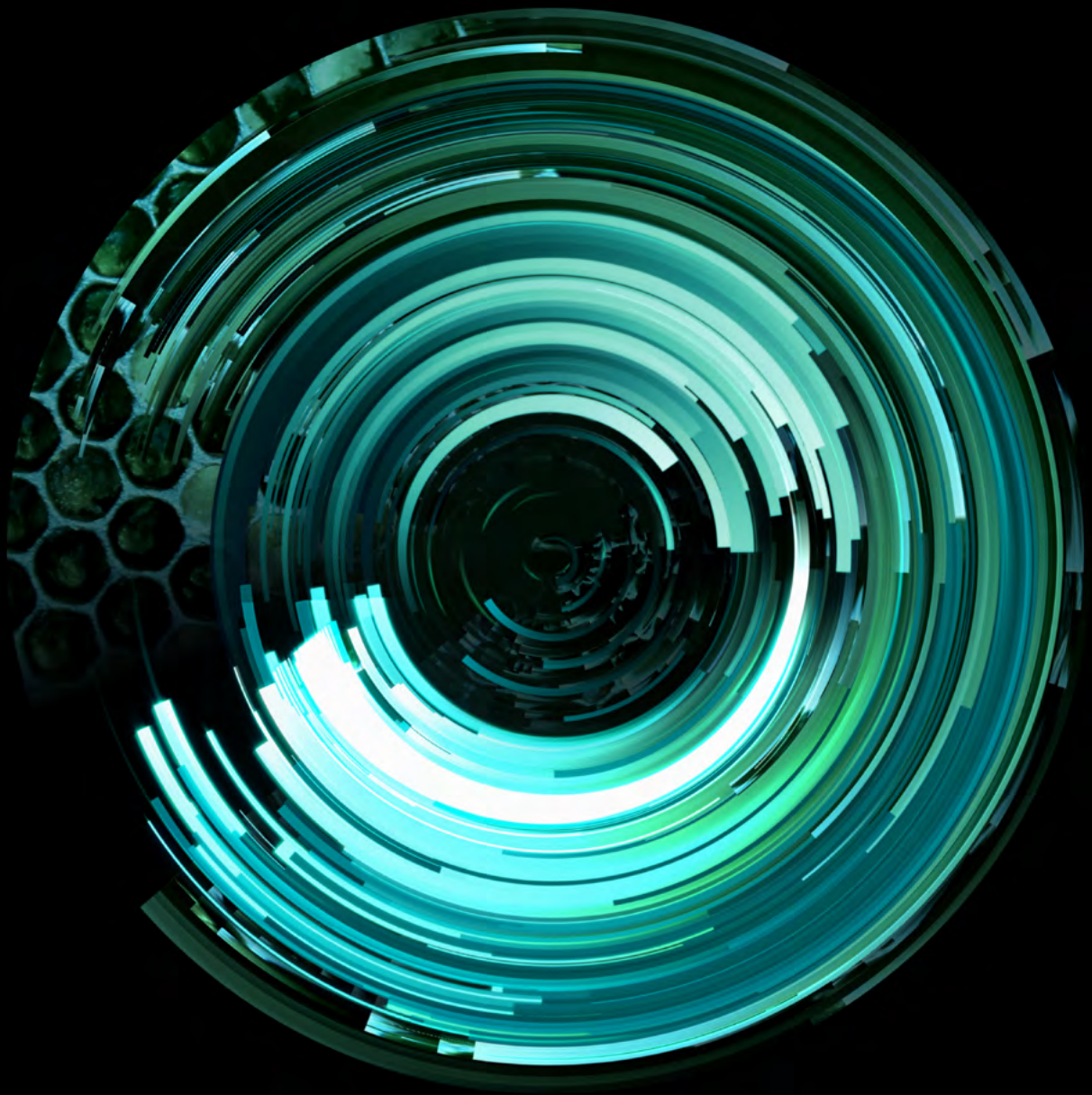
Deloitte.



Cloud Sovereignty

Succeeding in the evolving landscape

The Trident of Sovereignty

As more companies and government institutions migrate their workloads and data to the cloud, sovereignty has become increasingly significant. This shift demands a balanced approach that leverages the technological efficiency and innovation of the public cloud while minimizing reliance on external parties, ensuring control over the assets and operational autonomy.

While the EU has been at the forefront of the sovereignty debate, it has now become a global issue due to rising geopolitical and commercial tensions, such as those stemming from the post-COVID era, the Ukraine and Middle East conflicts, and intense China-US competition. This new context has heightened awareness in both the private and public sectors, as digital sovereignty is critical for navigating the complex regulatory landscapes and adopting cloud solutions that offer robust compliance mechanisms to address concerns about data privacy, technology supply chain vulnerabilities and uncertainty regarding where critical data is stored and processed in the cloud.

Cloud sovereignty interpretations can vary across regions and industries. However, a common challenge is the dominance of external Cloud Service Providers (CSPs) in certain regions. In the EU, for instance, AWS, Microsoft, and Google collectively hold a 70% market share. Furthermore, emerging technologies like AI can present additional challenges to achieving true sovereignty.

Drivers of sovereignty

Global & Regional crises

Government strategies

Data protection as focal point

Data Ecosystems

Challenges for Cloud Buyers

The drivers for genuine sovereignty can be classified into three domains:

Geopolitics: organizations need to navigate the complexities of global tensions and regional crises to maintain stable and secure cloud operations aligned with the agenda of government strategies

Regulation: organizations must adhere to regional- or industry-specific regulations to protect data privacy and security, with data protection as focal point, also in the context of new use cases from AI and data analytics (e.g.: Europe AI Act).

Market trends: organizations seek to achieve the benefits of emerging cloud technologies (e.g.: Generative AI, Edge) powered by the public cloud, balancing the need for control and operational transparency. Data ecosystems and interoperability are key to strengthening the industry and extending partnerships along the IT value chain to build software marketplaces.

Additionally, challenges persist for Cloud buyers related to the management of sovereign IT policies, control enforcement, operational transparency and security across vendors, spanning public, private cloud or on-premise environments.

Understanding and addressing all these challenges is essential for organizations to achieve a unified approach to cloud sovereignty, ensuring that technological transformation and governance of interconnected and distributed IT architectures reduce dependencies on external actors in a context of polarized geopolitics.

Some relevant facts

- The Ukraine – Russia conflict has activated massive data/application migration processes for Eastern Europe (e.g: data embassy for Estonia). Policymakers are also increasingly recognizing the importance of providing transparency and more control on the operational ecosystem. This acknowledgment extends beyond data sovereignty, highlighting clear dependencies in the software and infrastructure layers of sovereignty. These dependencies need to be regularly reviewed for realignment and to sustain cloud operational ecosystems.

- Within the regulatory framework, the impact of AI is becoming increasingly evident, especially in the countries with more dependencies on external parties. This development has driven the creation of the first horizontal AI regulation, the European AI Act. Adopted in 2024 by the European Parliament, it is recognized as the world's first comprehensive horizontal legal framework for AI. It establishes EU-wide rules on data quality, transparency, human oversight, and accountability. In terms of vertical regulation by industry, there is an increasing emphasis on regulating the operational ecosystem to ensure operational resilience and sovereign alignment.

- In the realm of market dynamics and due to the complexity of emerging technologies and their application in the industry, CSPs are making significant efforts to adjust their service offerings to these technologies, such as AI and Edge. The most notable progress is in enhancing the efficiency of the operational ecosystem, providing clients with greater control and transparency in operations. This advancement, in turn, facilitates the adoption of emerging technologies and builds more trust in the CSP sovereign capabilities.

Relevant examples

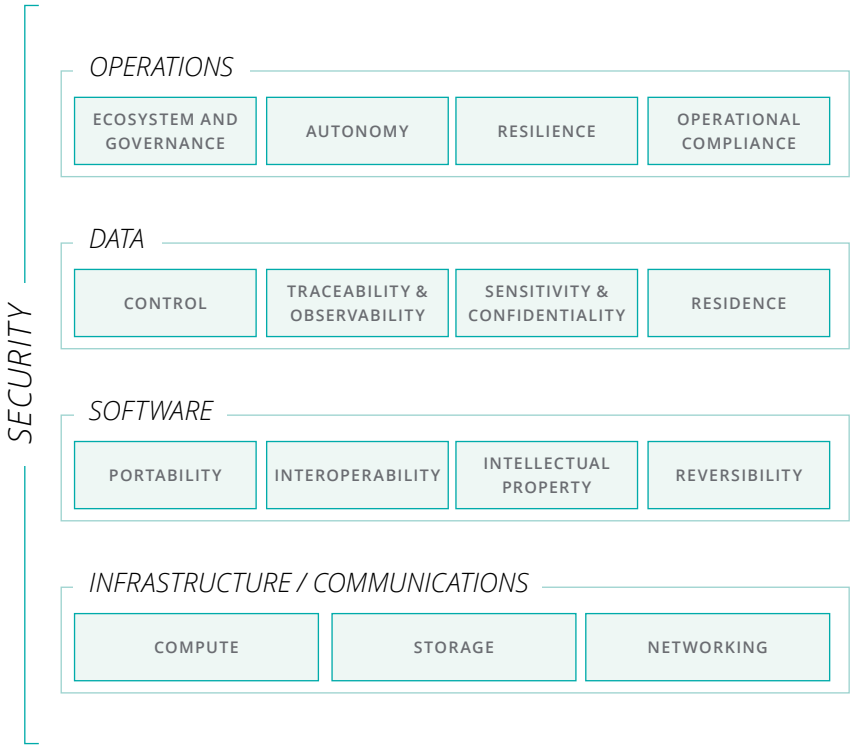
Nvidia & Oracle in Japan: NVIDIA to Help Elevate Japan's Sovereign AI Efforts Through Generative AI Infrastructure Build-Out.

G42 and e& in UAE: G42 AND e& will merge data center services under Khazna Data Centers.

First Data Embassy in the world: The Government of Estonia has approved the establishment of a network of Data Embassies.

Decoding Cloud Sovereignty

Cloud Sovereignty extends beyond data sovereignty, requiring a systemic view to ensure end-to-end compliance, data protection, and operational resilience across the full stack. Deloitte's framework considers five layers: Operations, Data, Software, and Infrastructure, with Security as a cross-layer.



Operational Sovereignty

Giving organizations visibility and control over provider operations drives operational resilience and prevents unauthorized data access. This is achieved by monitoring and controlling IT services and the underlying configuration items essential for securely and effectively delivering cloud services in alignment with sovereignty policies.

Benefits of operational sovereignty:

- **Transparency:** provides a complete view of the operational landscape and transparency, enabling better decision-making and building trust
- **Improved performance:** enhances the quality of operations through continuous monitoring and feedback.
- **Risk and compliance management:** proactively identifies and mitigates risks through policy automation, ensuring smooth and reliable operations for governance over the ecosystem.
- **Enhanced collaboration:** through seamless observability, it fosters better communication and collaboration across teams, aligning efforts towards operational goals.

Data Sovereignty

Ability to maintain control over the data, including storage location, protection methods, processing procedures, and access permissions. Full data sovereignty can only be achieved if the organization is the data owner. Otherwise, reliance on third-party agreements and contracts limits the degree of sovereignty attainable.

Benefits of Data Sovereignty:

- **Risk and compliance management:** reduces the risk of data breaches and unauthorized access by strictly controlling data handling processes, and ensures data storage complies with local laws and regulations.
- **Data lifecycle management:** provides a clear audit trail for all data activities from creation to deletion, enhancing traceability.
- **Control:** implements strict access controls to ensure only authorized personnel can access sensitive data, ensuring compliance and security.
- **Enhanced monitoring:** through data observability, continuous observation of data pipelines helps in identifying and resolving anomalies and incidents quickly.

Software Sovereignty

Ability of an organization to operate and orchestrate software or solutions independently without dependencies on a manufacturer's roadmap. This includes maintaining control over the IP, source code, development processes, and software updates, as well as the ability to shift between platform providers. Such solutions also provide the ability to be executed on many different platforms.

Benefits of Software Sovereignty:

- **Minimize technological dependencies:** reduces reliance on specific vendors or technologies, allowing organizations to gain technological sovereignty and avoid vendor lock-in so they can easily switch between platforms
- **Leveraging Open IP:** fosters collaboration and innovation within a defined digital ecosystem, protecting intellectual property.
- **Optimized platform engineering:** effective software sovereignty supports advanced platform engineering practices by ensuring that applications can be easily integrated across different environments.
- **Operational resilience:** ensures that organizations can easily transition during a technological migration and improve operational resilience based on reversibility.

Infrastructure Sovereignty

Infrastructure and communications are the technical foundations of sovereignty for the operations, data and software layers and enable control over them.

Utilizing open standards for infrastructure and communications maximizes adaptability and resilience to shift between sovereignty scenarios.

Benefits of Infrastructure Sovereignty:

- **Optimized storage solutions:** control over storage infrastructure ensures data can be stored and accessed efficiently and securely.
- **Improved communication networks:** sovereign networking infrastructure enables secure communication channels and reliable connections for business operations and data interoperability.
- **Confidential computing:** isolation and secure processing of workloads and data with hardware-based Trusted Execution Environments (TEEs) . Also applicable to GPUs in computing intensive tasks for AI, machine learning, and data analytics.
- **Sovereign edge:** networking and computing sovereignty are of special relevance for the edge to address data protection while maintaining optimal levels of operational and technological autonomy.

Security layer

Security acts as a cross capability which ensures robust protection and integrity across the operations, data, software, and infrastructure layers through comprehensive end-to-end security management.

Benefits:

- **Comprehensive management:** ensures robust E2E security management across all layers, addresses security dependencies, providing a cohesive and unified security posture
- **Threat detection and response:** allows organizations to implement advanced threat detection and response mechanisms in coordination with Governance, mitigating impact and ensuring continuous protection and compliance.

Cloud Sovereignty Across CSPs

POSITIONING

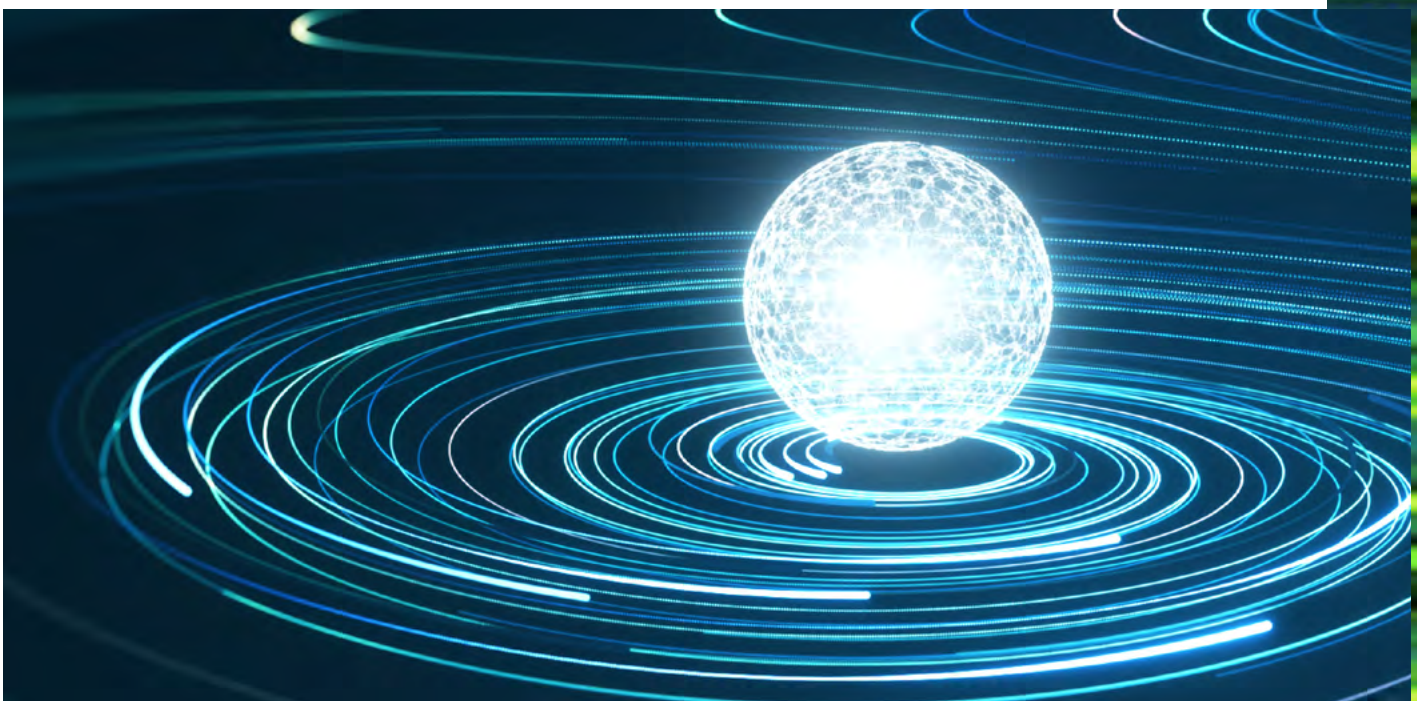
Amazon Web Services (AWS) offers the scale and the full power of cloud with their 'Sovereign by Design' approach, which they have continued to innovate on, and have announced new infrastructure and services to give their customers further choice in how to meet their unique sovereignty requirements.

The AWS Nitro System is the best example 'Sovereign By Design', a hypervisor to further protect and securely process highly sensitive data, is the foundation of AWS computing service Amazon EC2 and powers all AWS Regions. Nitro is designed to enforce restrictions so that nobody, including anyone in AWS, can access customer workloads on EC2.

AWS is enhancing its market position in sovereign Cloud with the AWS European Sovereign Cloud and AWS Dedicated Local Zones.

The AWS European Sovereign Cloud (ESC), the first region to be launched in Germany by the end of 2025, will offer a fully independent cloud, operated and supported by AWS personnel located in the EU to meet operational sovereignty requirements. This cloud will allow customers to keep all their data and the metadata they create within the EU, ensuring compliance with regional regulations and maintain the same architecture, service portfolio, and APIs as global regions and powered by the AWS Nitro system. Additionally, AI services such as Amazon Bedrock and Amazon Sagemaker, will be available.

Global AWS Dedicated Local Zones provide private cloud solutions via infrastructure that is fully managed by AWS and connected to its global public cloud. This infrastructure is built for exclusive use by a customer and placed in a customer-specified location. AWS Dedicated Local Zones offer limited service availability compared to the global public cloud. For instance, a recent AWS Dedicated Local Zone was launched in Singapore, developed in collaboration with the Singapore Government's Smart Nation and Digital Government Group (SNDGG) to meet stringent data isolation and security requirements, enabling sensitive workloads to run securely in the cloud.



PORTFOLIO AND GO TO MARKET

In the pursuit of operational sovereignty, AWS offers a wide range of tools and controls. For instance, Control Tower empowers organizations to implement automated guardrails, centralized logging, and industry-leading security best practices, ensuring operational control and compliance. Regarding automated guardrails, Landing Zones can be customized to address specific regulatory frameworks. Sovereign Controls (more than 240 available) in addition to hybrid infrastructure services like Outposts, also enable data residency and drive operational autonomy to guarantee adherence to stringent sovereignty regulation.

Additionally, the AWS Key Management Service grants customers granular control over encryption keys, safeguarding sensitive data. AWS also offers the option to encrypt keys outside AWS cloud using the KMS External Key Store (XKS), as part of their continued Sovereign-by-Design innovations. Complementary tools like Amazon Macie can identify data vulnerabilities, further strengthening data residency and sovereignty. Finally, Nitro Enclaves provide a hardware-based Trusted Execution Environment, isolating compute processing tasks and protecting infrastructure from unauthorized access.

COMPETITIVE ADVANTAGE

AWS stands out in the realm of cloud sovereignty due to its versatility, scalability, and extensive integration capabilities. AWS provides customizable compliance frameworks and dedicated sovereign cloud services to cater to specific regulatory requirements, ensuring that organizations can tailor their cloud environments to meet local data sovereignty laws. This flexibility allows users to determine their own risk levels and adjust their compliance and security measures accordingly, giving them more control and choice over their sovereignty navigation and the pace at which they adopt different levels of risk management.

With AWS's Sovereign-by-Design approach, customers have less complexities, because across AWS's choices of infrastructure and services, their customers benefit from the same architecture, expansive service portfolios and APIs.

Another significant competitive advantage of AWS is its resilience, supported by a robust global network. This global presence ensures that resources are readily available from various regions, providing robust disaster recovery and data portability options. Furthermore, AWS's capacity to integrate with third-party solutions (SaaS marketplace) enhxances its extensibility. AWS facilitates the integration of specialized third-party security tools, thereby ensuring compliance and security when specific regulations must be met, allowing AWS to offer customizable sovereignty solutions.

POSITIONING

Microsoft Azure is is strategically advancing its market position by expanding its global infrastructure and enhancing its hybrid edge capabilities in the Cloud continuum through a unified control plane (Microsoft Arc). Azure has invested in new data center regions worldwide to provide local compliance and low-latency services to customers. This includes the latest addition of the sovereign cloud regions Azure Government U.S. and Azure China, operated by local entities to meet specific regulatory requirements.

Microsoft Cloud for Sovereignty, a set of tools and features layered on top of the existing Microsoft Cloud services, allows customers to address data and operational sovereignty requirements swiftly by providing operational transparency and addressing heightened requirements for data residency, privacy, access control, and operational compliance.

PORTFOLIO AND GO TO MARKET

In its commitment to operational sovereignty, Microsoft Azure provides organizations with Sovereign Landing Zones, a variant of the enterprise-scale Azure Landing Zones, that allows to meet compliance requirements through Azure-native deployments via Infrastructure as Code (IaC) and Policy as Code (PaC). These guardrails simplify the architecture and deployment of security services and policy controls, and leverages automation to support compliance for public sector and government agencies.

To strengthen transparency and accountability in operations, Azure recently introduced Transparency Logs to provide customers with details of when Microsoft engineers access their resources (accessed subscriptions, time of access, service, etc.).

Furthermore, Azure tackles infrastructure sovereignty with Trusted Execution Environments (TEEs). These secure enclaves isolate the processing of sensitive or strategic data, adding an extra layer of protection. Customer-owned encryption keys are passed confidentially and securely directly from a managed hardware security module to the TEEs that work with the customer's encrypted data.

COMPETITIVE ADVANTAGE

Azure offers significant competitive advantages in the cloud sovereignty paradigm through its structured and comprehensive approach. Azure provides a streamlined pathway to achieving sovereignty goals and compliance, enabling organizations to get the best out of the public cloud with support for hybrid architectures. This approach is supported by unified resource management and Microsoft Arc as E2E control plane. Thus organizations can have data residency in public cloud environment with sovereignty controls, running hybrid services on-premises with additional operational controls, or running completely disconnected from global network.

Azure also excels in control lifecycle management with tools such as Policy Compiler, and Drift Analyzer, which are part of the Microsoft Cloud for Sovereignty suite. These tools are designed to detect policy overlaps and deviations against the baseline, adapting to the evolving needs of customers.

POSITIONING

Google Cloud provides a variety of control packages on its public and distributed cloud platforms to meet specific sovereignty requirements. These packages include software- and hardware-based, and partner-operated controls. For example, Google Sovereign Cloud Controls are implemented on a per-country basis to address data residency needs. These options are available not only in Europe but also in Asia and the Pacific.

To further demonstrate its commitment to the public sector, Google Public Sector has partnered with World Wide Technology (WWT) to introduce Google Distributed Cloud Hosted (GDC Hosted), a secure cloud solution tailored for US government agencies. This distributed cloud option offers a range of control packages, from on-premises to full disconnection, for end-user organizations and domestic service providers. GDC delivers Google Cloud's core infrastructure as a service (IaaS), including Kubernetes and advanced cloud services such as database and machine learning services, as well as a subset of services from Google's Vertex AI product.

PORTFOLIO AND GO TO MARKET

Google Cloud prioritizes operational sovereignty with Anthos and Anthos for Edge delivering a consistent platform for managing and deploying workloads across hybrid and multi-cloud environments, ensuring operational control and compliance (e.g. Config Manager and Policy Controller)

Data sovereignty is empowered by Assured Workloads providing strong data protection for their workloads to meet data residency and regulatory requirements.

Google Cloud's Confidential Computing features services like Confidential VMs and GKE Nodes (encrypted Kubernetes) to enhance infrastructure sovereignty by protecting data through hardware-based encryption from unauthorized access.

COMPETITIVE ADVANTAGE

Google Cloud offers a significant competitive advantage through its multicloud functionality with Google Kubernetes Engine Anthos as control plane, which allows for seamless deployment and management across different environments.

Config Sync, part of GKE, lets cluster operators and platform administrators deploy configurations from a source of truth. The service has the flexibility to support one or many clusters and automatically enforce compliance policies across all managed environments. This flexibility reduces vendor lock-in and provides consistent management and policy enforcement, enhancing operational efficiency.

Google Cloud's present a similar approach to deploy AI, allowing businesses to leverage advanced AI across distributed cloud platforms, ensuring scalability and accelerating innovation. The commitment to open-source technologies promotes technological sovereignty, providing transparency, survivability, easier KMS (key management) integrations and fostering a collaborative ecosystem.

Additionally, Google Cloud strategy with local partners is well defined for operating and overseeing sovereign controls in a shared responsibility model which facilitates sovereignty governance and compliance.

POSITIONING

Oracle Cloud provides public cloud services designed to meet organizational data sovereignty requirements. These services encompass the Oracle Commercial Public Cloud, available in multiple global regions to ensure compliance with disaster recovery and data residency regulations. In addition to the public cloud, OCI offers two specific Sovereign Public Clouds: Oracle EU Sovereign Cloud, serving both private and public sectors within the EU with a focus on regulated or regionally significant data and applications; and Government Cloud, customized specifically for government entities.

For organizations requiring on-premises solutions, OCI offers three different dedicated Cloud options. OCI Dedicated Region offers a complete OCI region in your own data center, ensuring all the commercial Public Cloud benefits. Oracle Cloud Isolated Region is designed for classified and mission-critical workloads, providing a secure environment for sensitive data. Lastly, Oracle Alloy enables partners to become Cloud service providers, extending a full range of cloud services to their clients ensuring data control and sovereignty.

PORTFOLIO AND GO TO MARKET

OCI focuses on delivering robust hybrid cloud solutions with a strong emphasis on security and sovereignty. The Compute Cloud@Customer service enables organizations to deploy Oracle's Exadata Database Service on-premises, ensuring operational sovereignty and compliance with data residency requirements.

Additionally, OCI's Sovereign AI addresses privacy concerns by providing AI and machine learning services that operate within specified geographic boundaries, offering organizations data privacy and regulatory compliance.

As for decentralized architectures, OCI's Roving Edge allows for local data processing and storage while seamlessly integrating with the central cloud for unified management and compliance. This capability supports low-latency deployment of OCI workloads in distributed environments, enhancing operational efficiency and data sovereignty.

Regarding Key Management Service, OCI further strengthens security with a centralized solution for managing and controlling encryption keys across its cloud services ranging from BYOK (Bring your own key) to BYOE (Bring you own encryption) as the highest control level by the customer in alliance with Thales as Hardware Security Module provider.

COMPETITIVE ADVANTAGE

Oracle distinguishes itself through its specialization in the public sector and industries with stringent sovereignty requirements. This focus ensures that organizations in highly regulated environments can meet rigorous compliance and data sovereignty mandates. OCI’s differentiated sovereignty realm-based architecture provides a robust framework for data isolation and control, enhancing security and compliance.

Additionally, OCI offers various Key Management Service (KMS) options, allowing organizations to select the one that best fits their specific needs, ensuring flexible and comprehensive data encryption and key management solutions that further secure sensitive information.

POSITIONING

OVH Cloud, as a European provider, is committed to ensuring cloud sovereignty by design and protecting the data hosted by its EU customers. The company implements technical and organizational measures to safeguard against interference from non-EU authorities, complies with EU regulations, and opposes requests that are not carried out in accordance with GDPR provisions. .

PORTFOLIO AND GO TO MARKET

As a provider of trusted cloud and data sovereignty, OVHcloud distributes 100+ services with different deployment models: Partnered with VMware to offer Hosted Private Cloud solutions, OVHcloud features the most certified VMware's offer in Europe in order to meet strict local regulations (e.g. SecNumCloud for French Government).

OVHcloud's Public Cloud is based on open-source standards and documented APIs and automation with focus on data protection, security, reversibility and transparency for cloud operations.

For strategic European data, OVHcloud has established Trusted Zones, which are designed to meet specific security and data sovereignty commitments. These zones are operated and supported exclusively by personnel located within the European Union.

Additionally, OVHcloud Confidential Computing adds a security layer by isolating sensitive data processing within secure enclaves and Nutanix-powered environments, further enhancing data protection within the infrastructure.

VMware solutions on OVHcloud are compliant with VMware Sovereign Cloud guidelines and other regulatory benchmarks.

Moving to the data layer, vSphere by VMware forms the foundation, offering a comprehensive platform for efficiently managing virtualized environments. Infrastructure sovereignty is enhanced via vSphere Native Key Provider, enabling local generation, storage, and management of encryption keys.

COMPETITIVE ADVANTAGE

OVHcloud, as a leading European provider in hosted private cloud, aligns closely with EU regulations for organizations seeking stringent data sovereignty and secure, compliant, and locally regulated cloud services. Its strong reputation in the public sector, demonstrated by national certifications such as SecNumCloud in France, ENS in Spain, C5 in Germany, ... underscores its commitment to security and regulatory adherence. These certifications ensure OVHcloud meets rigorous standards set by national cybersecurity authorities, offering a trusted and flexible solution for government and public sector entities.

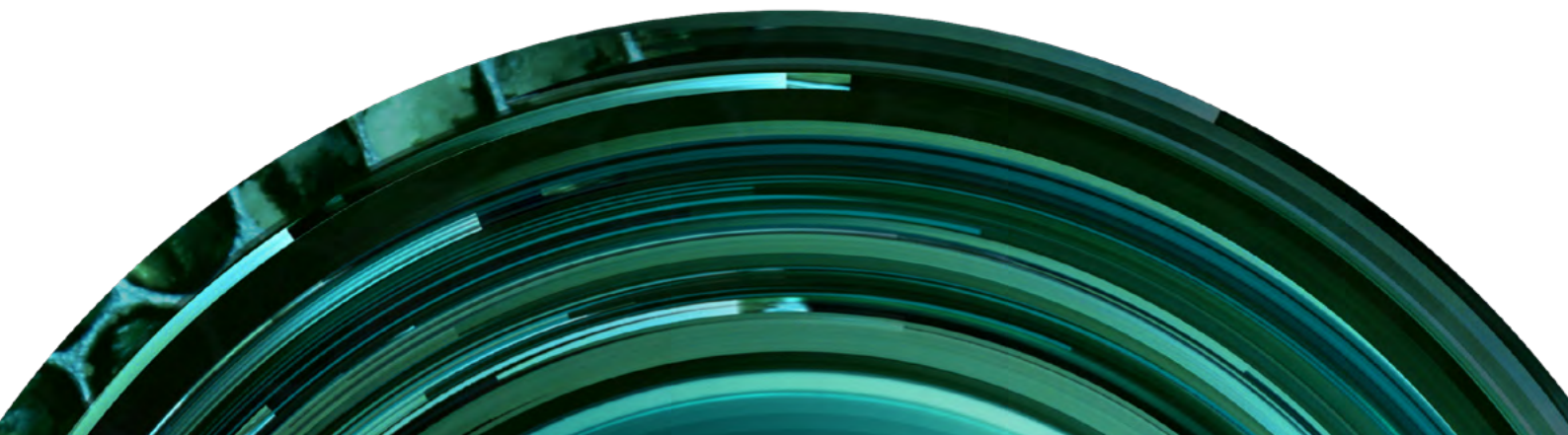
The future of Cloud Sovereignty

In the rapidly evolving landscape of digital ecosystems, maintaining control and compliance of cloud assets will be crucial for ensuring robust sovereignty. To navigate this complex terrain effectively, organizations will need to focus on three interconnected domains for a comprehensive strategy transcending data sovereignty

Embracing open architectures

Leveraging automation through Policy as Code

Implementing seamless observability



Open Architectures

Open architectures represent a design philosophy emphasizing openness, flexibility, and interoperability. This approach relies on publicly available standards, allowing different software and hardware components to integrate seamlessly. By adopting open architecture, cloud services can overcome proprietary limitations, fostering a more collaborative, adaptable, and innovative infrastructure.

Open architectures are also crucial for driving technological sovereignty by ensuring compatibility and interoperability among diverse systems and vendors. This approach simplifies integration and enables organizations to implement customized security measures tailored to their specific needs and regulatory requirements. It reduces reliance on proprietary solutions, promoting a dynamic and responsive sovereignty strategy.

For instance, OpenStack and OpenNebula exemplify open architectures, offering modular designs that allow enterprises to select and integrate the most suitable cloud components and services for their needs. These stacks and platforms also facilitate easy updates and replacements with minimal disruption, aligning with evolving compliance requirements.

As cloud sovereignty is an ongoing journey, open architectures will help organizations adapt to continuous changes driven by geopolitical shifts, regulatory updates, and market trends. They ensure that cloud environments remain compliant and secure despite uncertainty or unexpected external factors. This approach not only enhances operational resilience but also supports long-term strategic goals, enabling organizations to retain control over their cloud assets and avoid the constraints of vendor lock-in. Furthermore, by providing access to a broader range of solutions, open architectures often lead to more cost-effective and innovative options.

Automation in Sovereignty (Compliance as Code)

Automation also plays a pivotal role in enhancing cloud sovereignty by streamlining and standardizing the implementation of policies across cloud environments. Through automation, organizations can develop unified policies that ensure consistent governance and compliance, mitigating risks associated with dispersed, inconsistent, or overlapped policies.

Policy as code is the concept of writing code in a high-level language to manage and automate policies. By representing policies as code in text files, proven software development best practices can be adopted such as version control, automated testing, and automated deployment.

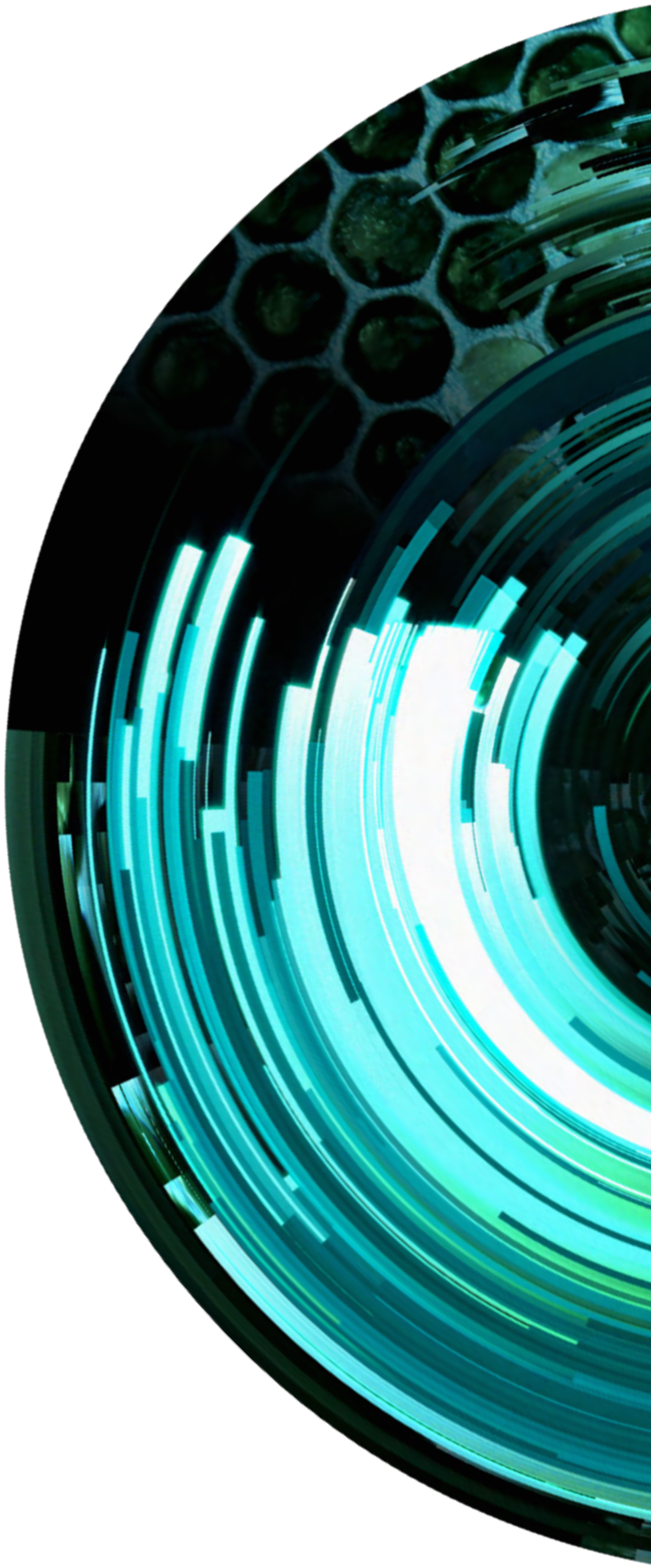
By adopting Policy as Code for sovereignty, enterprises can embed compliance checks directly into their development pipelines, automatically identifying and rectifying configuration drifts (data location, unauthorized access, etc.). This automated approach paves the way for real-time enforcement of sovereignty protocols, ensuring that cloud resources adhere to enterprise standards and regulatory requirements.

Automation also facilitates auditing, providing visibility into the sovereignty baseline of cloud assets. It can help remediate deviations from established policies, enabling automated corrective actions as well. This strengthens the overall sovereignty framework and, also empowers organizations to maintain control over their workloads and datasets.

Seamless observability

Seamless observability is essential for maintaining the openness and compliance necessary for a robust cloud sovereignty strategy. By offering comprehensive visibility into the entire cloud environment and its dependencies, seamless observability enhances organizations' technical capabilities in openness and automation. It enables effective monitoring, detection, and response to sovereignty issues across four key domains:

- **Dynamic sovereignty:** by eliminating proprietary constraints, open architectures foster a more adaptable infrastructure. Observability solutions monitor the dynamic environment, providing insights into how different components and systems interact and perform. This visibility allows organizations to identify pain points ensuring that their data and applications remain compliant despite evolving geopolitical or regulatory factors.
- **Vendor independence and innovation:** observability platforms aggregate data from various sources, offering a unified view of performance and compliance across different vendors and technologies. This holistic view supports better decision-making by identifying new opportunities and potential improvements to reduce dependency on specific vendors.
- **Unified and consistent governance:** observability also provides visibility into policy enforcement and compliance status across the entire cloud infrastructure. This ensures that all resources comply with established policies, facilitating consistent governance and reducing the likelihood of compliance gaps.
- **Continuous auditing and remediation:** Policy as Code facilitates continuous auditing by tracking policy compliance in real time. Observability platforms can leverage this data to provide insights into compliance status and identify any deviations. Automated remediation actions can be triggered to address non-compliance issues promptly, strengthening the sovereignty framework and ensuring that organizational standards are consistently met.



Conclusions

Initially launched as a European initiative, Cloud Sovereignty has grown to have global significance, prompting Cloud Service Providers (CSPs) to develop sovereign cloud solutions tailored to specific countries and regions beyond the EU. These offerings ensure that workloads and data comply with regional and industry-specific regulations, reflecting a shared commitment between customers and providers to address local sovereignty concerns.

CSPs are thus increasingly forming strategic partnerships with governments and local businesses to create customized solutions that meet stringent regional security and regulatory standards. These collaborations are crucial not only for technical compliance but also for the safe adoption of emerging technologies within a broader sovereignty framework that considers all the implications, including operational and technological autonomy.

As both governments and private organizations seek greater control over their cloud data and operations, CSPs will keep expanding and refining their sovereign cloud portfolios to balance the efficiency and innovation of public cloud services with the requirements for maintaining part of the infrastructure, applications, and data on-premises.

Navigating the diverse regulatory landscapes and the complexity of cloud-native architectures will require a thorough and strategic approach. It will be essential to reduce technological dependencies and streamline the management of the hybrid-edge cloud continuum through the adoption of open architectures, leveraging compliance automation, and benefit from advanced cloud observability capabilities to ensure an effective and seamless Journey to Cloud Sovereignty

Contacts

Alfons Buxó
Partner
abuxoferrer@deloitte.es

Bram De Schouwer
Partner
bradeschouwer@deloitte.com

Álvaro Martín
Senior Manager
amartindelvalle@deloitte.es

Abdul Hameed Tutakhail
Senior Manager
atutakhail@deloitte.com

Sebastien Scholaert
Senior Consultant
sscholaert@deloitte.com

Juan Carlos Cano Martín
Analyst
jcanomartin@deloitte.es

Deloitte.