CISPE Sovereignty & Resilience Framework for Cloud Services

"How do we ensure effective control of and access to our cloud data, infrastructure and services - especially in the event of interference by foreign governments or third parties?"

This is the question being asked in boardrooms around the world. The CISPE Sovereignty Framework answers with a certification scheme for individual cloud services. Using the framework, initially for self-declaration, with certification by independent expert third-parties within 6 months, vendors can confirm exactly which cloud services provide a satisfactory level of control either through Sovereignty or Resiliency, with an agreed, accepted and robust definition.

Sovereign and Resilient Badges. Sovereignty is about control. CISPE's Sovereignty Framework allows for two distinct, equally legitimate routes - based on freedom of choice - to demonstrate effective control over services, data and applications. Customers want assurance that their cloud services and data protected from interventions, curtailment and access from foreign governments and third parties. In addition, they also need to demonstrate ways to retain control over cloud data, infrastructure and services when needing to use services with non-sovereign elements, or to support operations and supply chains that cross more than one jurisdiction.

The CISPE Sovereign Cloud Service Badge provides clarity and assurance of control through ownership, control and legal jurisdiction in a defined geography.
The CISPE Resilient Cloud Service Badge demonstrates control through assessment of key factors that collectively deliver the level of control necessary to achieve strategic autonomy over digital services.

The CISPE Sovereignty Framework is based on the principle that effective control over cloud services, data and infrastructure can be achieved through both jurisdictional and technical means. Critically, the CISPE Sovereignty Framework assesses individual services, not vendors themselves.

Defined Geographical Area of Sovereignty: Every jurisdiction asserts its own sovereignty. To assess whether a cloud service and its provider meet sovereignty requirements in a specific geography, CISPE has introduced the concept of Defined Geographical Area of Sovereignty, extending the notion of "sovereign" services beyond Europe. Each Defined Geographical Area of Sovereignty corresponds to one specific jurisdiction that meets the common criteria defined under the CISPE Sovereignty Badge, enabling conformity to be assessed and compared across jurisdictions. In this way, the CISPE Sovereignty Framework extends beyond the Europe-only

recognition of sovereign services under existing Frameworks - such as those of Gaia-X Level 3 - to jurisdictions worldwide.

Importantly, the CISPE Sovereignty Framework is not a security, cybersecurity, or business continuity framework, nor does it replace existing ones. Instead, it builds on recognised security standards, including ISO standards, C5, ENISA guidance, NIS2, DORA, and other relevant frameworks.

I. CISPE Sovereign Cloud Service Badge

Awarded to a specified cloud service that has been certified as demonstrating sovereign ownership and control of a company providing such service within a specified and relevant jurisdiction (i.e. the European Union) and that the Critical Assets and data reside and are under exclusive control of parties in that same region.

The CISPE Sovereign Cloud Service Badge can be awarded solely to first-party services that independently satisfy the applicable sovereignty requirements. The fact that a provider offers, markets, or resells both sovereign and non-sovereign services shall not, in itself, affect eligibility. However, a service that does not itself meet the criteria for, and is not independently certified under, the CISPE Sovereign Cloud Service Badge shall not obtain such a badge through submission by a reseller or by association with another certified service.

As such, customers can select these services knowing that proven sovereignty provides the control they require over their data and applications. CISPE foresees that sovereignty labels may be awarded by other jurisdictions providing customers with further choice of services which they may consider as part of global trusted cloud solutions. We characterise these as Defined geographical areas of sovereignty (see above).

The mandatory requirements for the CISPE Sovereign Cloud Service Badge are detailed in Appendix 1: Sovereignty.

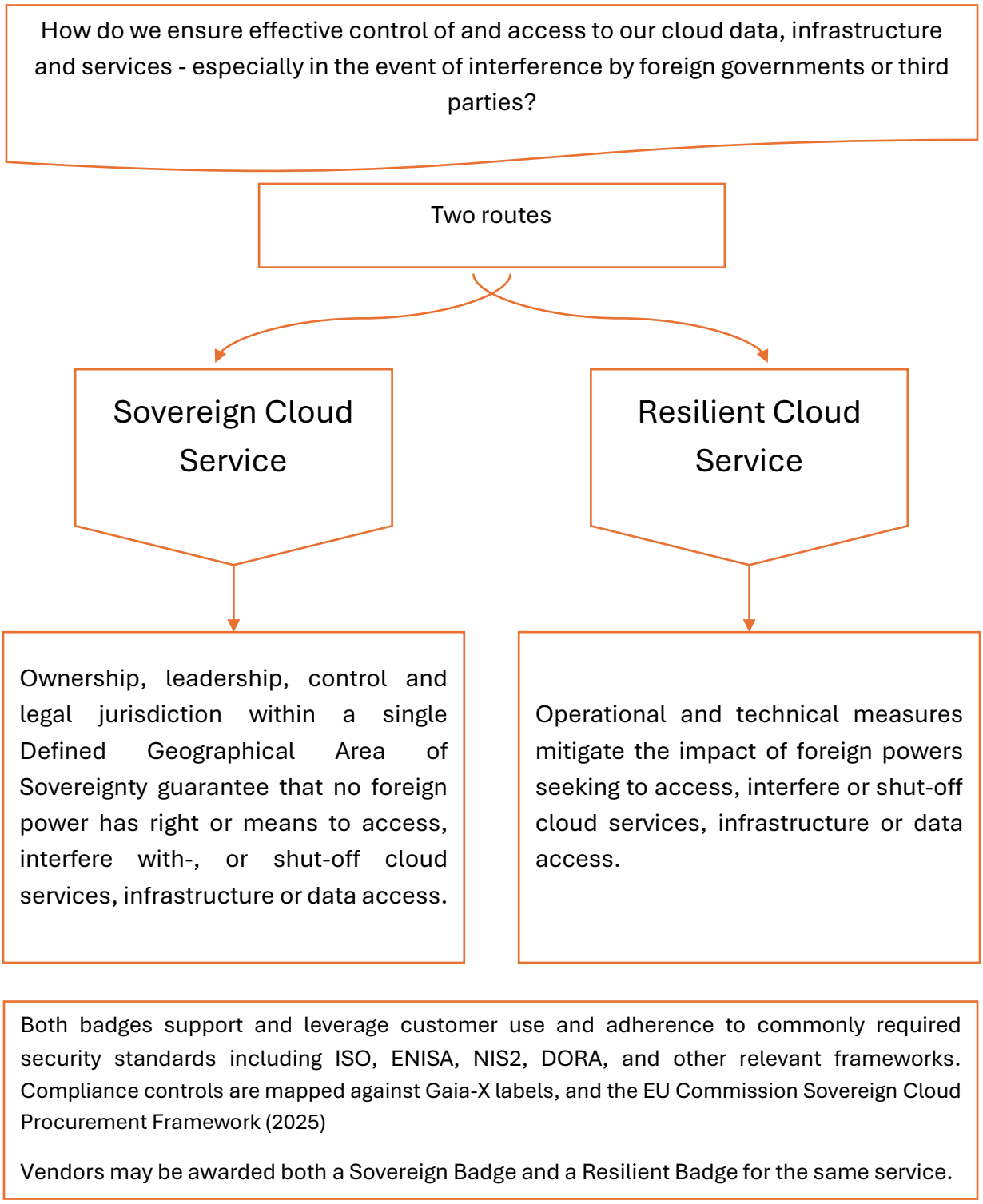
II. CISPE Resilient Cloud Service Badge

For customers who wish, or need, to purchase services that rely on elements which do not meet sovereignty requirements - either because they are provided by non-sovereign providers, or because they interact as part of global supply chains that cross more than one specified and relevant jurisdiction - the CISPE Resilient Cloud Service Badge provides a certified assessment of key factors that collectively deliver a level of control comparable to that of a sovereign service. These include data security and immunity from access through encryption and customer management of keys; demonstrated ability to access data in case of foreign government intervention; and redeployment of the service to an alternate provider.

As with the Sovereignty Badge, the CISPE Resilient Cloud Service Badge is awarded to a specific cloud service. Choosing a Resilient cloud service requires both the provider and its customers to implement additional technical and procedural steps that may increase the price of the service.

The mandatory requirements for the CISPE Resilient Cloud Service Badge are detailed in Appendix 2: Resilience.

Importantly, and as CISPE believes that core requirements for Sovereign and Resilient Cloud Services are binary in nature. However, in the future it aims to add a number of value-added



Both badges support and leverage customer use and adherence to commonly required security standards including ISO, ENISA, NIS2, DORA, and other relevant frameworks. Compliance controls are mapped against Gaia-X labels, and the EU Commission Sovereign Cloud Procurement Framework (2025)

Vendors may be awarded both a Sovereign Badge and a Resilient Badge for the same service.

elements to the Resilience Badge. These have the potential to be rated to reflect differing levels of resilience. These may prove valuable alongside existing procurement frameworks, such as the European Commission Sovereign Cloud Procurement Framework (2025).
In most circumstances the straightforward way for customers to maintain control over their data when faced with threat of interference from foreign governments will be to exclusively select services with the CISPE Sovereign Cloud Service Badge. However, the CISPE Resilient Cloud Service Badge provides a comparable level of control albeit requiring additional actions from both vendor and customer. This may be more suitable for certain services, workloads and situations.

Finally, it is entirely possible that vendors may seek and be awarded both a Sovereign Badge and a Resilient Badge for the same service. Whilst being under the legal control of a single jurisdiction may confer immunity from judicial overreach by a foreign power, Resilience offers additional safeguards that may be relevant or attractive for specific workloads.

CISPE Governance and Independence in Developing this Framework

For decisions specifically concerning the sovereignty of cloud providers and their services - and in particular for the development of the current Framework - CISPE has established a dedicated Sovereignty Committee. This committee is composed exclusively of European companies that meet the Legal Requirements on Sovereignty as defined in the CISPE bylaws. It serves as the ultimate decision-making body on sovereignty matters, ensuring that such decisions are taken solely by companies free from extraterritorial influence.

Overseas hyperscalers are not involved in the development of the CISPE Sovereignty Label. While these significant market players play an important role in meeting the needs of customers across Europe, the CISPE bylaws - amended by the General Assembly in February 2025 -explicitly ensure that hyperscalers neither hold voting rights nor occupy positions that could enable them to influence the organisation’s decisions or governance.

The following European companies are members of the in the CISPE Sovereignty Committee formulating this framework:

Anexia (Austria), Aruba (Italy), Leaseweb (Netherlands), NumSpot (France), OUTSCALE / Dassault Systèmes (France), Opiquad (Italy), Jotelulu (Spain), Infomaniak (Switzerland), Clever Cloud (France), OpenNebula (Spain), Deda Cloud (Italy), ReeVo (Italy), WaveCom (Estonia), oXya (France).

To support the development of this Framework, CISPE is assisted by specialist advisors, including BYCYB (formerly LNE), which is accredited by the French National Cybersecurity Agency (ANSSI) as a qualified body to audit and monitor compliance with the SecNumCloud certification. Such

certification represents the highest standards of cybersecurity and sovereignty practices for cloud service providers.

The Appendices below and provided as separate documents list all requirements applicable to both the Sovereignty and Resilience Badges, as well as definitions.

- Definitions – See below
- CISPE Sovereign Cloud Service Badge - Appendix 1
- CISPE Resilient Cloud Service Badge - Appendix 2

DEFINITIONS

1. **Administrative Data:** Data relating to the contractual relationship between the service provider and the customer, including:
   (i) KYC information;
   (ii) subscription and contract details;
   (iii) billing and financial data;
   (iv) payment information;
   (v) support data (support tickets, messages, attachments).
2. **Asset:** Any asset used by the service provider to provide the services, including physical assets (data centres, physical infrastructure, servers, etc.), digital assets (systems, applications, databases, etc.), and human assets (maintenance teams, support teams, etc.)
3. **Control Plane**: All infrastructures, core systems, and functions that configure, govern, secure, observe, meter, or update the service, including identity and access management (IAM), policy and authorisation systems, orchestration and service catalogues, configuration and state stores, logging, monitoring and telemetry, usage metering, PKI and key management systems, CI/CD pipelines and artefact registries, administrative consoles and APIs, and maintenance gateways. Control Plane components shall be operated in accordance with the Operational Autonomy and Software Autonomy requirements.
4. **Critical Assets:** Any asset, including people, systems, credentials, cryptographic material, software, or infrastructure, that is used to store and/or process Critical Data, and/or whose compromise could grant administrative control over, or visibility into, Critical Data. This includes, but is not limited to:

   – Data Plane components;
   – storage, compute, and network resources made available to the customer;
   – Control Plane components, including identity and access management and policy systems, orchestration and service catalogues, configuration and state stores, logging, monitoring and telemetry, metering, PKI, key management systems, hardware security modules and certificate authorities, CI/CD pipelines and artefact registries, administrative consoles and APIs, and maintenance gateways;
   – network and security controls (including SDN controllers, DNS, DHCP, IPAM, and secret stores);
   – identity and recovery systems (including directories, backup and restore orchestration, and update-signing and build keys).

5. **Critical Data:** For the purposes of this framework, the following data shall be considered Critical Data:
   (i) Customer's Data;
   (ii) Users Data;
   (iii) Technical Data – defined as any data, credentials, configurations, or information that may be used to access, manage, control, or otherwise affect Customer or User Data.

6. **Customer's data:** Data entrusted by the customer to the service provider, meaning data hosted and processed by the customer, or on its behalf, within the cloud infrastructure service provided to it, excluding Users Data, Technical Data, and Administrative Data.
7. **Data Plane:** The runtime environment, including compute, storage, and networking resources such as virtual machines, containers, volumes, object stores, databases, and load balancers, that executes customer workloads and persists Customer's Data and customer-generated metadata, including inputs and outputs
8. **Defined Geographical Area of Sovereignty:** A country or group of countries designated by the service provider, from the jurisdiction of which the service provider intends to demonstrate it is subject. A Defined Geographical Area of Sovereignty differs from a service availability zone or region, which refers to the geographical areas where the service provider's infrastructure, including data centres, is located.
9. **Failover:** The switching to an equivalent standby asset when the initial component can no longer technically operate or can no longer operate in compliance with the requirements of this framework.
10. **Federated and distributed cloud infrastructure service:** cloud computing

    Cloud computing services for compute, storage, networking, and higher-level digital services that are:
    (a) provided by multiple independent cloud service providers, each remaining legally and operationally responsible for its own infrastructure and services;
    (b) distributed, in that the underlying resources are deployed across multiple geographically distinct sites, including central, regional, and edge infrastructures within the Union; and
    (c) federated, in that such services are interoperable and jointly consumable through common governance rules, trust frameworks, and orchestration mechanisms.

    Federation shall be enabled through the use of open-source software components and open standards, including shared Control Planes, interoperable APIs, and resource-exchange mechanisms, which ensure portability and interoperability, including in accordance with Regulation (EU) 2023/2854 (Data Act) where applicable, prevent vendor lock-in, and allow participation on a non-discriminatory and transparent basis.

    Federation shall not require the transfer of operational control, administrative privileges, or software life-cycle authority outside the Defined Geographical Area of Sovereignty of each participating provider.

11. **Key hardware equipment and components:** Hardware equipment and components that are necessary to provide the service and whose unavailability would impact service continuity.
12. **Lock-in feature:** A feature that makes it prohibitively expensive, excessively technically complex, or unreasonably time-consuming for the customer to switch to another vendor, including due to platform features that make data migration and application re-engineering difficult and disruptive.
13. **Non-sovereign entity:** An entity that does not comply with the requirements set out in Appendix 1 of this framework, including entities subject to legal, contractual, or technical

control by third countries or entities outside the Defined Geographical Area of Sovereignty.

14. **Operational autonomy:** The service provider's continuous ability to operate, administer, secure, support, and restore the service exclusively from within the Defined Geographical Area of Sovereignty, without requiring access, approval, or intervention from any external entity outside that area.
15. **Software autonomy:** The service provider's independent control over the software life cycle of the service, in particular the Control Plane, including the rights and means to build, sign, validate, deploy, patch, and roll back software without vendor intervention outside the Defined Geographical Area of Sovereignty.
16. **Sovereign entity:** An entity that complies with the requirements set out in Appendix 1 of this framework.
17. **Technical Data:** All configuration, operational, and performance information generated or managed by the Control Plane to operate cloud infrastructure components, including compute, storage, and networking, such as:
    (i) resource identifiers and metadata (including resource identifiers, host-names, machine types, data centre regions, and resource status);
    (ii) hardware and software configuration;
    (iii) networking and topology data;
    (iv) usage and performance data;
    (v) storage and volume data;
    (vi) security information;
    (vii) life-cycle and integration data
18. **Users Data:** Data relating to the utilisation and management of the services, including:
    (i) user identification data such as names and email addresses;
    (ii) authentication data, including identifiers, passwords, certificates, IP addresses, and VPN information;
    (iii) access rights, including roles, permissions, and user preferences;
    (iv) login history, including IP addresses, timestamps, and browser information;
    (v) management and utilisation events, including creation, configuration, and deletion timestamps.

    Users Data may include personal data within the meaning of Regulation (EU) 2016/679, where applicable.

-Ends-