Cloud Sovereignty Framework

Implementation guidance

Introduction 1

Sovereignty Objectives 1

Sovereignty Effective Assurance Levels 2

Assessment of Sovereignty Objectives 3

The Sovereign Cloud Framework Matrix 6

Depth of analysis 12

Lessons learnt 13

Introduction

The Commission's Cloud Sovereignty Framework was first presented in October 2025 as part of a call for tenders launched under Cloud III Dynamic Purchasing System (Cloud III DPS) that aimed to procure sovereign cloud for the European Union institutions, bodies, offices and agencies. The Framework lays out criteria used to evaluate the sovereignty of the providers that applied to the call for tenders. It also shows how its two main components – the **Sovereignty Effectiveness Assurance Level (SEAL)** and the **Global Sovereignty Score** – were calculated.

This document is published at a time when the tender process implementing the framework has been successfully concluded. It aims to support public entities that intend to apply similar approach when assessing the level of sovereignty of digital services, and provide direction to providers who wish to achieve higher level of sovereignty and resilience. The document is complemented with a calculator, described in the present document, that provides information regarding the various computations performed in the context of the framework, based on the return on experience of the cloud tender.

For the sake of clarity, the text below includes the relevant excerpts from the original document in order to allow the reader to refer to this document alone.

Sovereignty Objectives

The list of Sovereignty Objectives of the framework is provided in the following table:

#	Sovereignty Objectives	Sovereignty Objective Descriptions
SOV-1	**Strategic Sovereignty**	Strategic sovereignty captures the degree to which a cloud provider (or technology actor) is anchored within the European Union/EEA legal, financial, and industrial ecosystem. It assesses ownership stability, governance influence, and alignment with EU strategic priorities.

#	Sovereignty Objectives	Sovereignty Objective Descriptions
SOV-2	**Legal & Jurisdictional Sovereignty**	Legal & Jurisdictional sovereignty evaluates the legal environment, exposure to foreign authority, and enforceability of rights that govern a technology provider and its services. It determines the extent to which a provider is anchored in European jurisdiction and insulated from external legal claims.
SOV-3	**Data & AI Sovereignty**	Data & AI sovereignty focuses on the **protection, control, and independence of data assets and AI services** within the EU/EEA. It addresses how data is secured, where it is processed, and the degree of autonomy customers retain over AI capabilities.
SOV-4	**Operational Sovereignty**	Operational sovereignty measures the **practical ability of EU actors to run, support, and evolve a technology independently of foreign control**. It focuses on continuity of operations, skill availability, and resilience against external dependencies.
SOV-5	**Supply Chain Sovereignty**	Supply chain sovereignty evaluates the **geographic origin, transparency, and resilience of the technology supply chain**, focusing on the extent to which critical components and processes remain under EU control or exposed to non-EU dependencies.
SOV-6	**Technology Sovereignty**	Technology sovereignty evaluates the **degree of openness, transparency, and independence in the underlying technological stack**, ensuring EU actors can interoperate, audit, and evolve solutions without lock-in to foreign proprietary systems.
SOV-7	**Security & Compliance Sovereignty**	Security & Compliance sovereignty measures the **extent to which security operations, compliance obligations, and resilience measures are controlled within the EU**, ensuring independence from foreign jurisdictions and long-term operational assurance.
SOV-8	**Environmental Sustainability**	Environmental sustainability assesses **autonomy and resilience** of cloud services over the long term in relation to **energy usage, dependency and raw material scarcity**.

Sovereignty Effective Assurance Levels

The detailed list of **Sovereignty Effectiveness Assurance Levels** (**SEAL**) relevant for the framework is provided in the table below:

Sovereignty Effectiveness Assurance Levels	Sovereignty Objective Descriptions
SEAL-0	**No** Sovereignty: Service, technology or operations under **exclusive control of non-EU third parties**, governed entirely by **non-EU jurisdictions**.
SEAL-1	**Jurisdictional** Sovereignty: **EU law formally applies** with **limited practical enforceability**; service, technology or operations under exclusive control of non-EU third parties.
SEAL-2	**Data** Sovereignty:

	EU jurisdictions apply, with **material dependencies remain**; service, technology or operations under indirect control of non-EU third parties.
SEAL-3	**Technological** Sovereignty: **EU jurisdictions apply**, EU actors exercising **meaningful but not full influence**; service, technology or operations under marginal control of non-EU third parties.
SEAL-4	**Full** Digital Sovereignty: Technology and operations under complete EU control, subject only to EU jurisdiction, with no critical non-EU dependencies.

Assessment of Sovereignty Objectives

The framework aims at assessing sovereignty according to eight Sovereignty Objectives. In the context of public procurement, the assessment performed by the Contracting Authority is based on the answers of the bidders, supporting documents provided with the answers, and public information made available by the provider. The quality assessment performed on the questions involved and used in the computation of the Sovereign Score are considered for the assessment.

Criteria involved in the assessments are described in the following table; questions and assessment are described more in detail in later sections of the document:

#	Sovereignty Objectives	Criteria
SOV-1	Strategic Sovereignty	• Ensuring that ultimate decision-making authority resides within EU jurisdiction, • Evaluating the likelihood of takeover or transfer to non-sovereign owners, measuring the capacity of EU stakeholders to shape the provider's technological and service evolution. • Degree to which the provider relies on EU-based financing rather than external capital. • Extent of investment, jobs, and value creation within EU/EEA. • Involvement in EU initiatives, Consistency with digital, green, and industrial sovereignty objectives defined at EU level. • Ability to sustain secure operations even if vendor support is withdrawn or disrupted.
SOV-2	Legal & Jurisdictional Sovereignty	• The national legal system governing the provider's operations and contracts. • Degree of exposure to non-EU laws with cross-border reach (e.g., US CLOUD Act, Chinese Cybersecurity Law). • Existence of legal, contractual, or technical channels through which non-EU authorities could compel access to data or systems. • Applicability of international regimes, which may restrict usage or transfer.

#	Sovereignty Objectives	Criteria
		• Location of intellectual property creation, registration, and development (EU vs. third countries), legal jurisdiction where IP rights are owned and enforced.
SOV-3	Data & AI Sovereignty	• Ensuring that only the customer, not the provider, has effective control over cryptographic access to their data. • Visibility into when, where, and by whom data is accessed, including auditability of AI model usage, mechanisms guaranteeing irreversible removal of data, with verifiable evidence. • Strict confinement of storage and processing to European jurisdictions, with no fallback to third countries. • Extent to which AI models and data pipelines are developed, trained, hosted, and governed under EU control, minimizing dependence on non-EU technology stacks.
SOV-4	Operational Sovereignty	• Ease of migrating workloads or integrating with alternative EU-controlled solutions without vendor lock-in. • Capacity for EU operators to manage, maintain, and support the technology without requiring non-EU vendor involvement • Existence of an EU-based talent pool with the expertise to operate and sustain the service. • Assurance that operational support is delivered from within the EU and subject exclusively to EU/EEA legal frameworks • Availability of full technical documentation, source code, and operational know-how enabling long-term autonomy. • Location and legal control of critical suppliers or subcontractors involved in service delivery.
SOV-5	Supply Chain Sovereignty	• Geographic source of key physical parts, manufacturing Location - countries where hardware is manufactured or assembled • Jurisdiction and provenance of embedded code controlling hardware, firmware • Origin of Software: where and by whom software is architected and programmed, location and jurisdiction governing software packaging, distribution, and updates. • Degree of reliance on non-EU vendors, facilities, or proprietary technologies • Visibility into the entire supplier and sub-supplier chain, including audit rights.
SOV-6	Technology Sovereignty	• Ability to integrate with other technologies through well-documented and non-proprietary APIs or protocols, extent to which the solution adheres to publicly governed and widely adopted standards, reducing dependency on single vendors

#	Sovereignty Objectives	Criteria
		• Whether software is accessible under open licenses, with rights to audit, modify, and redistribute, ensuring transparency and adaptability • Visibility into the design and functioning of the service, including architectural documentation, data flows, and dependencies • Degree of European independence in high-performance computing capabilities, including processors, accelerators, and software ecosystems.
SOV-7	Security & Compliance Sovereignty	• Attainment of EU and internationally recognized certifications (e.g., ISO, ENISA schemes) • Adherence to GDPR, NIS2, DORA, and other EU frameworks • Security Operations Centres and response teams operating exclusively under EU jurisdiction, control over security monitoring/logging - customer or EU authority ability to oversee logs, alerts, and monitoring functions directly. • Transparent, timely, and EU-compliant reporting of breaches or vulnerabilities, maintenance Autonomy - ability to develop, test, and apply security patches independently of non-EU vendors • Capacity for EU entities to perform independent security and compliance audits with full access.
SOV-8	Environmental Sustainability	• Adoption of energy-efficient infrastructure (e.g., low PUE) and measurable improvement targets. • Circular economy practices ensuring reuse, refurbishment, and responsible end-of-life treatment of hardware. • Transparent measurement and disclosure of carbon emissions, water usage, and other sustainability indicators. • Sourcing of renewable or low-carbon energy to power infrastructure and operations

The Sovereign Cloud Framework Matrix

This section is an instruction for reading the new sections of the document, and the attached calculator.

Please check the table below, and refer to the corresponding section to have a detailed explanation of the various elements of the calculator:

			Sov Score	68%	
		SEAL (Sovereignty Effective Assurance Level)			**SEAL-2**
Objective #	Description	Level/answers	Value	Score	SEAL
SOV-1 Strategic Sovereignty	Strategic sovereignty captures the degree to which a cloud provider (or technology actor) is anchored within the European Union/EEA legal, financial, and industrial ecosystem. It assesses ownership stability, governance influence, and alignment with EU strategic priorities.		20%	533	
		4. Non-EU authorities requests to access data or systems are disputed by the provider and eventually in some cases are accepted with customers being notified	125		1
		Non-EU authorities requests to access data or tems are always rejected by the provider	167	167	4
4	Export Control Restrictions - applicability of international regimes such as ITAR or EAR, which may restrict usage or transfer.	Restrictions exists towards a EU MS	-		0
		Restrictions exists towards EU citizens or international organisations	42		1
		Share of revenues >50% in the EU	84		3
		Part of the offer cannot be exposed to restrictions towards EU MSs	125	125	3
		Part of the offer cannot be exposed to restrictions towards EU MSs or international	167		4
5	Origin of IP - location of intellectual property creation, registration, and development (all).	1. Entirely outside the EU	-		4
		2. Mostly outside the EU	42		4
		3. Mixed within/outside the EU	84	84	4
		4. Mostly within the EU	125		4
		5. Fully within the EU	167		4
6	IP Holder Jurisdiction - legal jurisdiction where IP rights are owned and enforced.	non-EU law, one single country	-		3
		non-EU law, mixed non-EU countries	42		3
		Mixed law, some EU	84	84	4

1 This part is the Cloud Sovereignty Framework, split in Sovereignty Objectives. Each objective is further split in several **Specific Objectives** which will be accompanied by one or more questions. It is also indicated how much the score in each category weights in the final score calculation of the sovereignty mark.

Objective #	Description	Score (examples)
SOV-1 Strategic Sovereignty	Strategic sovereignty captures the degree to which a cloud provider (or technology actor) is anchored within the European Union/EEA legal, financial, and industrial ecosystem. It assesses ownership stability, governance influence, and alignment with EU strategic priorities.	Weight: 20%
SOV-2 Legal & Jurisdictional Sovereignty	Legal & Jurisdictional sovereignty evaluates the legal environment, exposure to foreign authority, and enforceability of rights that govern a technology provider and its services. It determines the extent to which a provider is anchored in European jurisdiction and insulated from external legal claims.	Weight: 10%
SOV-3 Data & AI Sovereignty	Data & AI sovereignty focuses on the protection, control, and independence of data assets and AI services within the EU/EEA. It addresses how data is secured, where it is processed, and the degree of autonomy customers retain over AI capabilities.	Weight: 10%
SOV-4 Operational Sovereignty	Operational sovereignty measures the practical ability of EU actors to run, support, and evolve a technology independently of foreign control. It focuses on continuity of operations, skill availability, and resilience against external dependencies.	Weight: 15%
SOV-5 Supply Chain Sovereignty	Supply chain sovereignty evaluates the geographic origin, transparency, and resilience of the technology supply chain, focusing on the extent to which critical components and processes remain under EU control or exposed to non-EU dependencies.	Weight: 10%
SOV-6 Technology Sovereignty	Technology sovereignty evaluates the degree of openness, transparency, and independence in the underlying technological stack, ensuring EU actors can interoperate, audit, and evolve solutions without lock-in to foreign proprietary systems.	Weight: 15%
SOV-7 Security & Compliance Sovereignty	Security & Compliance sovereignty measures the extent to which security operations, compliance obligations, and resilience measures are controlled within the EU , ensuring independence from foreign jurisdictions and long-term operational assurance.	Weight: 15%
SOV-8 Environmental Sustainability	Environmental sustainability assesses autonomy and resilience of cloud services over the long term in relation to energy usage, dependency and raw material scarcity.	Weight: 5%

2 The detailed guidelines to evaluate the Specific Objectives. The levels have a short specific description. For each specific objective there is a list of proposed answers, each associated with a certain score.

Objective #	Description	Level/answers
SOV-1 Strategic Sovereignty	Strategic sovereignty captures the degree to which a cloud provider (or technology actor) is anchored within the European Union/EEA legal, financial, and industrial ecosystem. It assesses ownership stability, governance influence, and alignment with EU strategic priorities.	
1	EU/EEA legal entity control - ensuring that ultimate decision-making authority resides within EU jurisdiction.	1. Entirely outside the EU
		2. Mostly outside the EU
		3. Mostly within the EU
		4. Entirely within the EU
2	Change of Control Risk - evaluating the likelihood of takeover or transfer to non-sovereign owners	1. Very likely
		2. Likely takeover by or transfer to a non-EU sovereign entity
		3. Somewhat likely takeover by or transfer to a non-EU sovereign entity
		4. Unlikely takeover by or transfer to a non-EU sovereign entity
		5. Very unlikely
3	Control Over Roadmap - measuring the capacity of EU stakeholders to shape the provider's technological and service evolution.	1. No influence possible
		2. Through "voice of the customer" public channels (e.g. feedback portals, online communities)
		0
		3. Governance bodies exist with EU actors participation
		4. Full influence of EU actors
4	Financial independence from non-EU capital - degree to which the provider relies on EU-based financing rather than external capital.	1. Almost entirely relying on non-EU funding
		2. Mostly relying on non-EU funding
		3. Balanced mix of EU and non-EU funding
		4. Majority of funding is EU-based
		5. Entirely EU-based funding
5	EU economic contribution - extent of investment, jobs, and value creation within EU/EEA.	1. Minimal
		2. Some
		3. Balanced EU/non-EU
		4. Majority in the EU

3 The same answers are used to determine the **SEAL** of each row, with each answer defining the SEAL level of the question. The evaluator ultimately decides whether the guaranteed sovereignty level corresponds to the framework proposal. When all responses grant SEAL-4, it must be understood that the criterion has no impact on the SEAL calculation.

		SEAL (Sovereignty Effective Assurance Level)			**SEAL-2**
Objective #	Description	Level/answers	Value	Score	SEAL
SOV-1 Strategic Sovereignty	Strategic sovereignty captures the degree to which a cloud provider (or technology actor) is anchored within the European Union/EEA legal, financial, and industrial ecosystem. It assesses ownership stability, governance influence, and alignment with EU strategic priorities.		20%	533	
1	EU/EEA legal entity control - ensuring that ultimate decision-making authority resides within EU jurisdiction.	1. Entirely outside the EU	-		1
		2. Mostly outside the EU	42		1
					3
		3. Mostly within the EU	83		3
		4. Entirely within the EU	125	125	4
2	Change of Control Risk - evaluating the likelihood of takeover or transfer to non-sovereign owners	1. Very likely	-		4
		2. Likely takeover by or transfer to a non-EU sovereign entity	31		4
		3. Somewhat likely takeover by or transfer to a non-EU sovereign entity	63	63	4
		4. Unlikely takeover by or transfer to a non-EU sovereign entity	94		4
		5. Very unlikely	125		4
3	Control Over Roadmap - measuring the capacity of EU stakeholders to shape the provider's technological and service evolution.	1. No influence possible	-		2
		2. Through "voice of the customer" public channels (e.g. feedback portals, online communities)	42	42	2
		0			3
		3. Governance bodies exist with EU actors participation	83		3
		4. Full influence of EU actors	125		4
4	Financial independence from non-EU capital - degree to which the provider relies on EU-based financing rather than external capital.	1. Almost entirely relying on non-EU funding	-		4
		2. Mostly relying on non-EU funding	31		4
		3. Balanced mix of EU and non-EU funding	63		4

The overall SEAL level is **the lowest SEAL level achieved in any of the objectives.**

SEAL (Sovereignty Effective Assurance Level)	**SEALx**

It is important to emphasize the prevalence of the SEAL criterion over the Sovereignty Score. In the context of cloud services procurement, the Contracting Authority decides what is the minimum SEAL required. Sovereignty score is used to compare the offers that have reached the minimum required SEAL.

The table below shows the main requirements met by each level from SEAL-2, which was the minimum level set for the competition:

	SEAL 2- Data Sovereignty: EU jurisdictions apply, with material dependencies remain; service, technology or operations under indirect control of non-EU third parties.	**SEAL 3 - Technological Sovereignty:** EU jurisdictions apply, EU actors exercising meaningful but not full influence; service, technology or operations under marginal control of non-EU third parties.	**SEAL 4 - Full Digital Sovereignty:** Technology and operations under complete EU control, subject only to EU jurisdiction, with no critical non-EU dependencies.
SOV-1 Strategic Sovereignty	An autonomous entity in its organization, but not in its technical choices. The service continues but no longer has access to updates and security patches in the event of a break in access to the underlying technology.	Access to the roadmap. Complete guarantee of operations continuity.	Decision-making centres exclusively in the EU. Priority European customers in roadmap arbitrations.
SOV-2 Legal & Jurisdictional Sovereignty	Isolation by creating separate entities. Limited exposure to export control-type measures.	Complete insulation guaranteeing the inapplicability of non-EU legislation. No exposure of Member States to export control measures.	Operations are designed and carried out exclusively in the EU. Protection of international institutions against export control measures.
SOV 3 Data & AI Sovereignty	Full control of the data, including encryption control, data localization and deletion guarantee. Logs available.	EU design AI. Logs recorded in real time in the EU.	Immutability of logs, audits carried out by European teams.
SOV-4 Operational Sovereignty	Operations carried out and documented locally. Expertise from outside the EU may be necessary. Open and documented alternatives exist.	Availability of expertise in Europe, including subcontractors. Processes are designed and documented locally.	Complete European autonomy, including security clearances and the integration of key skills of subcontractors.
SOV-5 Supply Chain Sovereignty	Majority of the supply chains are documented. Deployments are carried out locally, according to procedures that can be external. Critical suppliers and subcontractors can be audited.	The majority of services are designed in the EU. They are deployed and orchestrated locally. No subcontractors involved in critical services.	EU-certified components origin. EU design, build and compliance check. No dependence on non-EU suppliers. Complete auditability of suppliers and subcontractors.
SOV-6 Technology Sovereignty	The services are partially interoperable. HPC is hosted on-premises.	European and public standards for core services. Open-source majority and predominance of European contributors. Auditability of the architecture.	Full compliance: EU Open AI, public standard, open source.
SOV-7 Security & Compliance Sovereignty	EAL2 level security. Local operations, transparent and immediate feedback of information, audits allowed.	ELA 3.	EAL 4-5, ENISA integration, immutable logs
SOV-8 Environmental Sustainability	Documented and transparent approach.		EU-certified lifecycle, EU-audited reporting.

4 In the calculator, each answer is awarded a score, that can be adapted by contracting authorities. Values provided are values taking into account the return of experience of the tender where it is has been first used. Each Sovereignty Objective has in a final score. The total score is the consolidation of the Sovereignty Objective scores according to their respective weights. The calculator provides more detail on the applied formula.

			Sov Score	68%
		SEAL (Sovereignty Effective Assurance Level)		
Objective #	Description	Level/answers	Value	Score
SOV-1 Strategic Sovereignty	Strategic sovereignty captures the degree to which a cloud provider (or technology actor) is anchored within the European Union/EEA legal, financial, and industrial ecosystem. It assesses ownership stability, governance influence, and alignment with EU strategic priorities.		20%	533
1	EU/EEA legal entity control - ensuring that ultimate decision-making authority resides within EU jurisdiction.	1. Entirely outside the EU	-	
		2. Mostly outside the EU	42	
		3. Mostly within the EU	83	
		4. Entirely within the EU	125	125
2	Change of Control Risk - evaluating the likelihood of takeover or transfer to non-sovereign owners	1. Very likely	-	
		2. Likely takeover by or transfer to a non-EU sovereign entity	31	
		3. Somewhat likely takeover by or transfer to a non-EU sovereign entity	63	63
		4. Unlikely takeover by or transfer to a non-EU sovereign entity	94	
		5. Very unlikely	125	
3	Control Over Roadmap - measuring the capacity of EU stakeholders to shape the provider's technological and service evolution.	1. No influence possible	-	
		2. Through "voice of the customer" public channels (e.g. feedback portals, online communities)	42	42
		0		
		3. Governance bodies exist with EU actors participation	83	
		4. Full influence of EU actors	125	
4	Financial independence from non-EU capital - degree to which the provider relies on EU-based financing rather than external capital.	1. Almost entirely relying on non-EU funding	-	
		2. Mostly relying on non-EU funding	31	
		3. Balanced mix of EU and non-EU funding	63	
		4. Majority of funding is EU-based	94	94

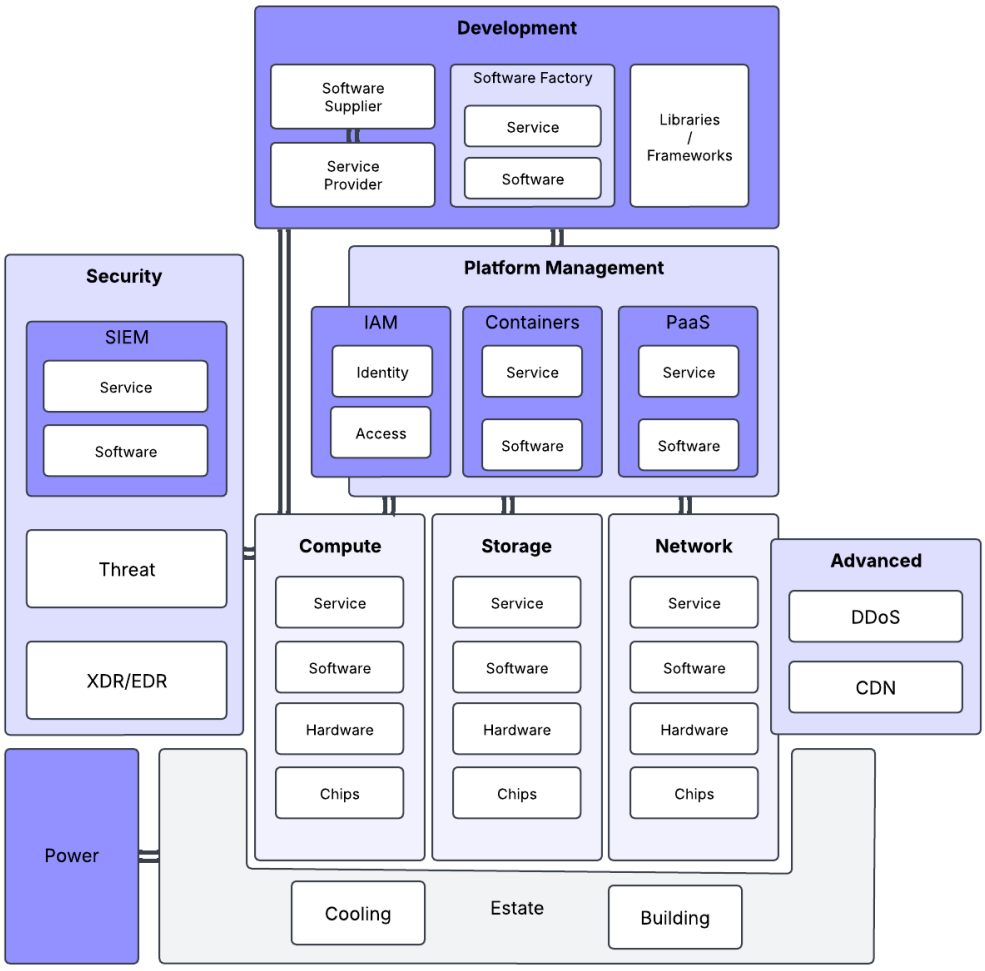
Depth of analysis

The Contracting Authority used the Sovereign Cloud Framework in the procurement procedure to assess the sovereignty of the offers. As such, the framework is generic, however it enables the Contracting Authority to gather detailed information on the cloud providers that will allow for a comprehensive and efficient assessment,

The information based on which the SEAL levels and the sovereignty score will be determined is therefore asked across:

- **all sovereignty dimensions;**
- **all the technical layers**, to identify all the hidden dependencies and supply chain.

The diagram below depicts the technical dimensions which are typically asked in the context of a cloud IaaS/PaaS tender such as the tender in progress:



Only through its extensive analysis, the contracting authority can get assurance that its sovereignty objectives are fulfilled. The evaluation must not stop at the level of the legal entity

which applied to the tender but all its chains of sub-contractors[1] and suppliers[2]. This approach allows to address the variety of solutions that the market creates. It also allows to investigate the sovereignty of all supplies such as third-party hardware or open-source that could be controlled by entities that could impair sovereignty objectives of the contracting authorities.

The sovereignty assessment, in the version of the framework used for this first tender is composed of 43 questions spread other the sovereignty objectives. On these 43 questions (corresponding to the points of interest of each sovereignty objectives listed in section 3.4), 9 are targeting solely the contractors and sub-contractors entities and covered most of the strategic and jurisdictional dimensions, while 19 questions are asked for every technical dimensions. This deep analysis of the technical dimensions allows Contracting Authority to investigate in depth any potential non-sovereign part of a solution and take it into account in the global sovereignty score.

In parallel, the SEAL levels evaluation takes into account this analysis, but it focuses on critical aspects that must be guaranteed in each technical dimensions for critical services. The Contracting Authority can decide on this list of critical services based on their needs. However, these should at least comprise the foundation technical layers such as compute, storage, network, security, IAM and critical PaaS services.

Lessons learnt

In the version of the Sovereignty Framework, we identified the following limitations that could be fixed in further iterations. We consider that the most relevant are:

- The level SEAL-4, however relevant, since it describes the highest level of Sovereignty, is not today relevant in the context of EU Sovereignty considering existing dependence to specific supply chains (chips, hardware). Relaxing the level SEAL-4, at least temporarily, would allow to make more difference between providers, especially when it comes to sensitiveness to hostile take-overs.

- However, we consider the framework was instrumental in the success of identifying sovereign solutions, relying on self-assessment and self-declaration requires a significant effort for contracting authorities during the evaluation of the declaration of the bidders. Further standardising the questions and the evidence to provide would certainly relieve the contracting authority from this workload.

For future assessment of sovereignty of IT supplies or services, we foresee to update the procedure based on these lessons.

[1] Sub-contractors : legal entities involved in the delivery of the contract

[2] Suppliers : legal entities that delivers supplies (hardware, software…) but that are not involved in the delivery of the service other than for technical support reasons triggered by contractors and sub-contractors involved in the delivery of the service. Suppliers never have access to infrastructure without supervision of the contractors.