Abilian
ECON LAB

Measure Twice, Buy Once

The Cloud and AI Development Act's Union assurance levels against the Commission's own SEAL scale, criterion by criterion, and eight amendments for the trilogue

Stefane Fermigier (Abilian) · sf@abilian.com · 18 September 2026 · DRAFT POSITION PAPER

Executive summary

The European Commission maintains two graded measures of cloud sovereignty. They do not correspond. The **Cloud Sovereignty Framework** scores a service on a Sovereignty Effectiveness Assurance Level, SEAL-0 to SEAL-4, across eight objectives, and takes the lowest of those scores as the verdict. The Commission built it for its own sovereign-cloud tender, set SEAL-2 as the floor, and has already chosen suppliers with it. Annex II of **the Cloud and AI Development Act** sets four Union assurance levels, which the Council and the Parliament are now examining and which will decide what every European public body may lawfully buy. Both instruments talk in levels. A buyer who reads one as a translation of the other will be wrong in both directions.

A service recognised at **Union assurance level 4**, the top of the Regulation's scale, can score **SEAL-0**, the bottom of the framework's. Annex II states no criterion on open standards, where the framework's worst answer scores zero. A service at **SEAL-4** is not guaranteed to reach **Union assurance level 2**, because the framework nowhere asks for the software bill of materials (SBOM) that Annex II makes a criterion.

Three consequences bear on the text now before the Council and the Parliament.

- **Article 30(3) admits a SEAL-1 service for the Union's public-order workloads**, which include the sectors of the NIS2 Directive [7], national security, defence, justice and law enforcement. At Union assurance level 2 a provider under the control of a third country qualifies by documenting mitigations. On the framework's first question that same provider answers that decision-making authority sits outside the Union, which scores SEAL-1. The lowest score is the verdict, so the whole assessment is SEAL-1. The Commission's own tender would have excluded the service at its floor.
- **Article 30(2) requires only Union assurance level 1 for every other public sector activity.** The provider assesses that level itself under Article 19. Its criteria admit a provider controlled from a third country, screened on one legal feature: whether a law of that country compels vulnerability reporting to its authorities before exploitation is known.
- **Of the 39 questions in the Commission's assessment that can lower a service's score, 14 are reached by an Annex II criterion, 8 appear only as audit evidence with no criterion behind them, and 17 are reached nowhere.** The Regulation says nothing about open standards, interoperability, a customer's ability to leave a supplier, or where hardware was designed and built.

Section 8 sets out eight amendments to the Commission text. These three give the most leverage per line of drafting.

1. **Promote into Annex II the supply-chain criteria that Annex III already contains.** Audit criterion I(2) restates four of the framework's supply-chain questions near-verbatim, as evidence an auditor collects with nothing to test it against. The text exists and needs moving.
2. **Extend the effective-control test of level 4 down to level 3.** That test asks whether a third country can materially influence a software component's technical evolution, maintenance priorities and long-term continuity. No other provision in Annex II reaches the question. A buyer without the answer cannot know whether an alternative supplier exists.
3. **Add an exit criterion at level 2 and above.** Chapter VI of the Data Act already obliges every provider in the Union to offer documented methods of export. Restating that as an assurance criterion gives an auditor something to test and imposes no new obligation on a compliant supplier.

About this note

The Cloud Sovereignty Framework was presented in October 2025 with the Cloud III Dynamic Purchasing System tender; its implementation guidance and sovereignty assessment calculator followed once that tender had concluded [2]. Its eight sovereignty objectives are numbered SOV-1 to SOV-8. A question inside one of them is cited here as SOV-n.m, in the calculator's own order. Annex II of the Cloud and AI Development Act (CADA) sets four Union assurance levels, the criteria a cloud provider must meet in order to sell to Union entities and public sector bodies at all [1].

This note compares them criterion by criterion: which requirement of one corresponds to which requirement of the other, at which level, and where no correspondence exists. Section 4 gives the full crosswalk, one row for each of the 48 questions in the Commission's own sovereignty assessment calculator. Section 5 works five concrete service profiles through both scales. Section 8 turns the findings into amendments.

Method. The SEAL side is read from the published calculator: every answer to every question has a SEAL value. The guidance states, as the spreadsheet implements, that a service's SEAL is the lowest value across all of them. The CADA side is read from Annexes II and III of COM(2026) 502 final and from the articles that operate them. One coding rule is applied to every row. A SEAL question is reached by **Annex II at level *n*** where *n* is the lowest Union assurance level whose cumulative criteria are inconsistent with every answer the calculator scores below SEAL-4. It is reached by **Annex III only** where the audit-evidence annex asks for evidence on the subject and Annex II states no criterion behind it. It is reached **nowhere** otherwise. Nine questions score SEAL-4 on every answer, so they cannot lower a SEAL level and the comparison does not arise for them. Annex A sets out the borderline calls.

Scope. The sources are the Commission proposal with its annexes and the two framework documents. Parliament and Council amendments are not in those sources, so every drafting reference here is to the Commission text. Two earlier lab positions on this proposal ask for amendments that this note does not repeat; section 9 lists them.

Findings

1. **Neither scale contains the other.** A service recognised at Union assurance level 4, the top of the Regulation's scale, is consistent with SEAL-0, the bottom of the framework's. Nothing in Annex II constrains the answer to SOV-6.2, open standards, whose worst answer scores SEAL-0. In the other

direction a service at SEAL-4 is not guaranteed to reach Union assurance level 2, because SEAL nowhere requires the software bill of materials that Annex II 2.1(i)(i) makes a criterion.

2. **Of the 39 SEAL questions that can lower a SEAL level, 14 are reached by an Annex II criterion, 8 appear only as Annex III audit evidence with no criterion behind them, and 17 are reached nowhere.** Three of the eight objectives have no Annex II criterion at all: supply chain, technology (openness, standards, interoperability, architecture, high-performance computing) and environmental sustainability, weighted 0.30 of the Commission's score between them. Environmental sustainability is reached by neither annex.
3. **The level Article 30(3) permits for the Union's public-order workloads scores SEAL-1.** At Union assurance level 2 a provider under the control of a third country qualifies by documenting mitigations. On SOV-1.1 that provider answers that ultimate decision-making authority sits mostly or entirely outside the Union, which scores SEAL-1. The minimum rule then extends SEAL-1 to the whole assessment. The Commission set SEAL-2 as the floor of its own tender.
4. **The level Article 30(2) requires for everything else is self-declared and open to a third-country-controlled provider.** Union assurance level 1 is assessed by the provider itself under Article 19. Its criteria admit a provider controlled from a third country, subject to one specific screen: that no law of that country requires vulnerability reporting to its authorities before exploitation is known.
5. **Hardware is excluded from Annexes II and III by a scope clause, which removes exactly the questions SEAL cannot answer either.** The framework's four hardware questions are SOV-5.1, SOV-5.2, SOV-5.3 and SOV-6.5. Three have no counterpart in the Regulation and SEAL neutralised the fourth, SOV-5.3, in its own calculator; the Commission's own lessons-learnt section says SEAL-4 is "not today relevant" because of dependence on chips and hardware. The Regulation does not resolve the problem. It defines the problem away. Article 32(3)(d) then returns hardware origin as a non-price award criterion that Article 32(2)(d) forbids to be decisive.
6. **Annex III has already imported four of SEAL's supply-chain criteria, near-verbatim, as evidence with no criterion behind it.** Audit criterion I(2) restates SOV-5.4, SOV-5.5, SOV-5.6 and SOV-5.7, narrowed from suppliers to software manufacturers. Evidence an auditor collects cannot fail a service that no criterion obliges. Promoting those four lines into Annex II is the cheapest amendment in this note. Its text is already drafted.
7. **The exit channel is absent from the Regulation and present in the framework.** SOV-4.1 reaches its top answer at "standard documented methods for data export", a bar Chapter VI of the Data Act already sets [4]. Annex II contains no portability or interoperability criterion at any level. A supplier's rent is bounded by what leaving would cost the buyer [8]. The Regulation certifies a supplier without ever measuring that cost.
8. **The two instruments measure certification on incommensurable scales.** Annex II (e) refers to European cybersecurity certification assurance levels under Regulation (EU) 2019/881 [5]; SOV-7.1 scores Common Criteria evaluation assurance levels (EALs). No mapping between them is published by either document.

1. The two instruments

Table 1 sets the two instruments side by side.

	Union assurance levels (CADA Annex II)	SEAL (Cloud Sovereignty Framework)
Legal status	Binding criteria in a proposed Regulation	Administrative framework, used in one tender, published as guidance

	Union assurance levels (CADA Annex II)	SEAL (Cloud Sovereignty Framework)
What it labels	A named cloud service of a named provider, with its subcontractors	An offer, across all technical layers and down the supplier chain
Scale	4 levels, no zero	5 levels, 0 to 4
What defines a level	A cumulative list of criteria, (a) to (k)	A statement about residual non-EU control, instantiated per objective
Aggregation	Conjunction: all criteria of the level, and by Article 20(1) of every level below	Minimum over 48 question scores
Second output	None	A weighted score in [0, 1], used to rank offers above the floor
Who assesses	The provider itself at level 1 (Art. 19); an accredited auditing organisation at levels 2 to 4 (Art. 20)	The contracting authority, on bidder self-declaration, supporting documents and public information
Recognition	Union-wide, by a national competent authority, with a cross-border objection procedure (Art. 17)	Per procurement
Who pays	The provider, for the audit, annually (Art. 20(1), 20(8))	The contracting authority, in evaluation effort
Scope of matter	Software in scope; hardware excluded by the Annex II scope clause	Hardware, firmware, software, operations, supply chain
Environmental	Absent	One of eight objectives, weight 0.05

Table 1. The two instruments side by side.

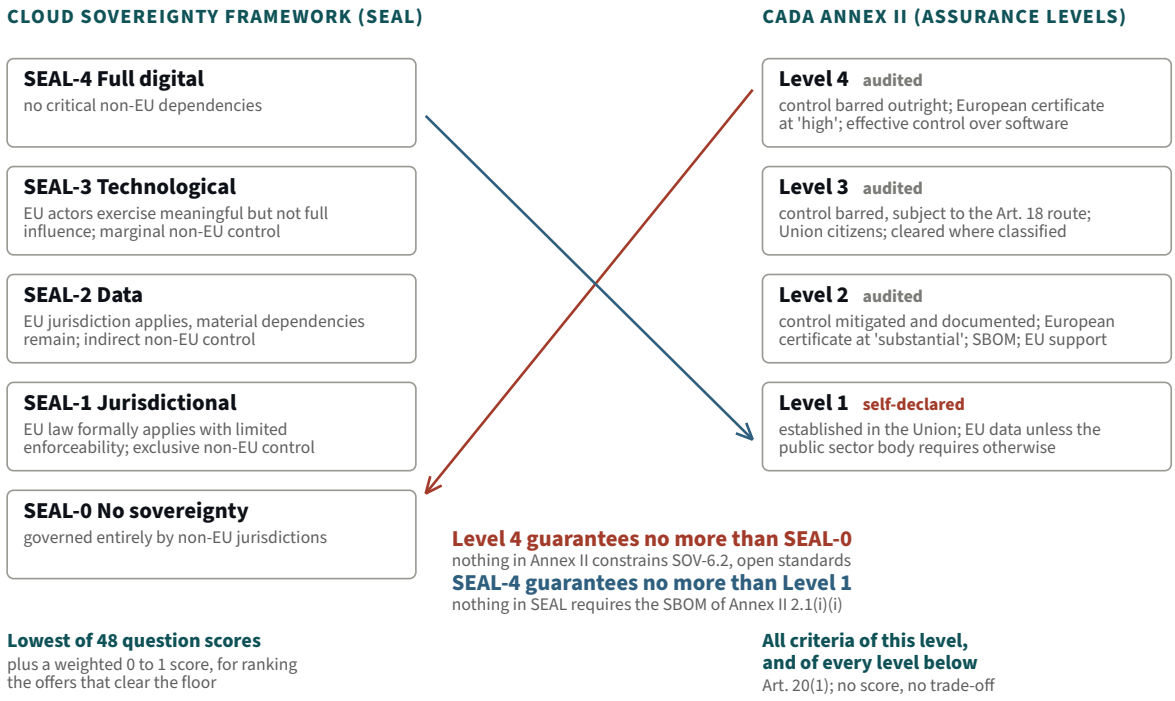


Figure 1. Each scale states its own rungs and its own aggregation rule. The two connectors mark the claims of section 2, each drawn in the colour of the claim it states: Union assurance level 4 guarantees no more

than SEAL-0 on the Commission's scale, and SEAL-4 guarantees no more than Union assurance level 1 on the Regulation's. Both claims are about criteria. Recognition at level 1 additionally requires the Article 19 procedure.

Two design choices in that table do most of the work. The Regulation is conjunctive and its levels nest: Article 20(1) provides that a provider audited at a higher level must satisfy every criterion of the levels below, and that failure at a lower level precludes the higher one. The framework is also conjunctive, over a different index set: eight objectives and their questions, aggregated by taking the minimum. The framework then adds a score, because a procurement has to rank the offers that clear the bar. The Regulation has no score, because a label does not rank.

2. Neither scale contains the other

The claim of finding 1 is checkable in both directions.

Union assurance level 4 is consistent with SEAL-0. Any one of three independent witnesses suffices under the minimum rule.

- SOV-6.2, open standards. Its worst answer is "core services (identity and access management, data formats, messaging, security, logging, integration protocols) rely mainly on proprietary technologies", which scores SEAL-0. Annex II states no criterion on open standards at any level. Annex III asks the audited provider to "provide a list of open standards that are followed" (I(3)(d)), which constrains nothing about what is on the list.
- SOV-6.1, open interfaces. Worst answer "integrations rely on closed or proprietary interfaces and formats controlled by the vendor", SEAL-0. No counterpart in Annex II.
- SOV-3.1, customer control of encryption keys. Worst answer "provider only", SEAL-0. Neither annex states a key-control criterion; the word "encrypted" appears in Annex III only to confirm that encryption does not excuse a transfer out of the Union.

SEAL-4 is not guaranteed to reach Union assurance level 2. A service at SEAL-4 has satisfied nothing in the framework that corresponds to Annex II 2.1(i)(i), the software bill of materials, nor to 2.1(i)(iii), the guarantee about third-country vulnerability-reporting law, nor to 2.1(f), which forbids data generated by using the service to train or fine-tune any AI system operated from a third country. SOV-3.5 asks where an AI service comes from, which is a different question from what the provider may do with the customer's data.

The two scales therefore imply nothing about each other. Neither document says so, and the shared vocabulary of levels invites the inference that they correspond.

3. The Union assurance levels by criterion

Table 2 states what each lettered criterion requires at each level. The crosswalk of section 4 is read against it.

Criterion	Level 1	Level 2	Level 3	Level 4
(a) Establishment	Provider established in the Union	Provider **and subcontractors** established in the Union	as level 2	as level 2
(b) Infrastructure, assets, personnel	Infrastructure and assets in the Union,	Infrastructure, assets and **personnel**	as level 2	as level 2

Criterion	Level 1	Level 2	Level 3	Level 4
	unless the buyer requires otherwise	in the Union, no override		
(c) Customer data, metadata, telemetry	Exclusively in the Union, unless the buyer requires otherwise	same	same	Data a risk assessment identifies as **sensitive**, exclusively in the Union, no override
(d) Personnel	No requirement. Instead: outsourced support outside the Union permitted with traceability, security and governance measures	Screening and Union citizenship **only if the buyer determines them necessary**	Personnel are **Union citizens**; national security clearance where classified information is handled	as level 3
(e) Cybersecurity	"State-of-the-art cybersecurity standards", no certificate required	European cybersecurity certificate at least **'substantial'** under Reg. 2019/881 [5], national schemes until one exists	as level 2	at least **'high'**
(f) Data and third-country AI	Absent	Data generated by using the service is not used to train or fine-tune any AI system operated from a third country, and is not transferred out	same	same
(g) Third-country control	**Permitted.** Only requirement: no third-country law compelling vulnerability reporting before exploitation is known	**Permitted if mitigated**: demonstrate measures preventing restraint on delivery, third-country access to data, disruption or degradation, and compelled compliance with foreign restrictive measures	**Prohibited**, with a derogation where the Commission has adopted an implementing act; under it, "reasonable access to the code" is added	**Prohibited**, no derogation
(h) Support	Covered by (d) above	Technical and operational support, including sub-outsourcing, initiated and performed **exclusively within the Union**	as level 2, **by Union residents** and by third parties not under third-country control	as level 3

Criterion	Level 1	Level 2	Level 3	Level 4
(i) Software supply chain	Absent	(i) SBOM and dependency list; (ii) controls blocking remote features that could tamper during updates, source-code audits of security-relevant third-country components, a documented migration plan; (iii) the vulnerability-law guarantee	as level 2	SBOM; and **no third-country effective control over the design, development, maintenance and evolution** of components, defined as the ability to materially influence technical evolution, maintenance priorities, security remediation and long-term continuity
(j) Open-source software	Absent	Documented controls preventing use of remote features that could tamper with or disrupt a device, system or software	same	same
(k) Subsidiaries	Absent	Effective legal, technical and organisational separation between the Union parent and any third-country subsidiary	same	same
Subcontractors covered	First tier, direct contractual relationship	same	same, **plus** those that may require access to classified or sensitive information	same as level 3
Assessment	**Self-assessment**, EU statement of conformity, published (Art. 19)	Independent third-party audit, annual review (Art. 20)	same	same

Table 2. The eleven criteria of Annex II at each Union assurance level. Bold marks what changes from the level to its left. "Same" means the criterion is kept unchanged, which Article 20(1) requires in any case.

Four discriminators define the four levels. Who is covered: the provider, then the provider and its subcontractors. What happens to third-country control: tolerated, then mitigated, then prohibited with a derogation, then prohibited. Who the people are: no requirement, then located in the Union, then Union citizens and cleared. What is asked of the software supply chain: nothing, then an SBOM with tamper controls, then effective control over the component's evolution.

Level 1 is a different kind of object from levels 2 to 4. Its criteria are lettered (a) to (g) where the others run (a) to (k). The letters do not align: level 1's (d) is about outsourced support, while level 2's (d) is about personnel. Level 1 speaks of "the cloud computing service provider" where every higher level speaks of "the audited provider". All eleven audit criteria in Annex III are stated to apply to "Union assurance levels 2, 3, and 4". Level 1 sits outside the audit annex entirely. Article 19 makes it a self-assessment with a published statement of conformity. Where the provider is an SME, Article 17(3) recognises that statement automatically across the Union.

The override clause in criterion (c) defeats the criterion it sits in. "Unless the public sector body explicitly requires otherwise" appears four times: on infrastructure and assets at level 1, and in the data-residency criterion at levels 1, 2 and 3. Recognition under Article 17 is of a service, Union-wide. By Article 20(1) the criteria of the lower levels apply upward, so the override survives at level 4 for data a risk assessment has not identified as sensitive. A criterion a single public sector body can switch off is a criterion an auditor cannot test.

4. The crosswalk

Figure 2 plots the result. Each cell is one question of the Commission's sovereignty assessment, coloured by where the Regulation reaches it.

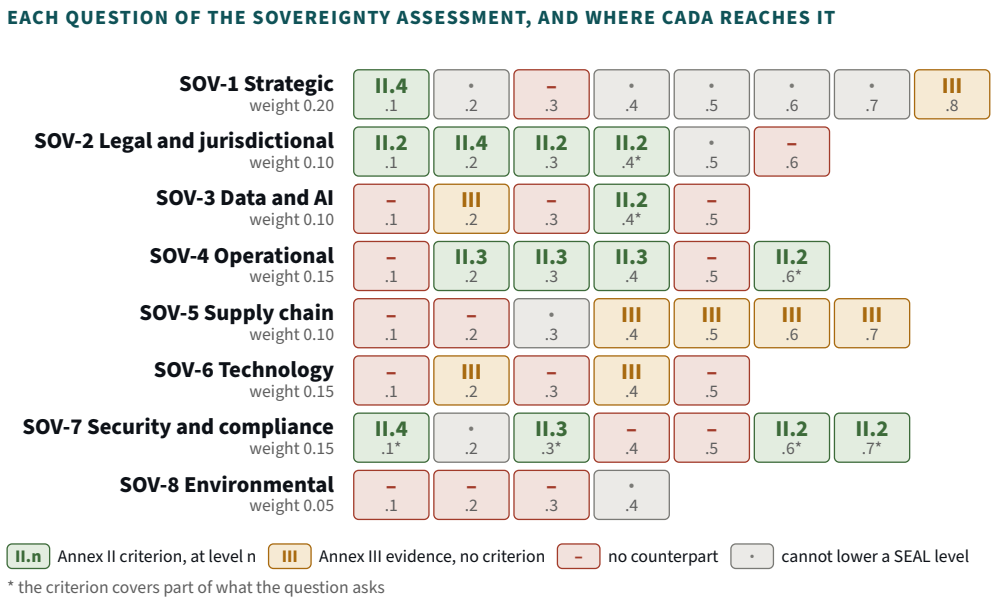


Figure 2. Where the Regulation reaches each question of the sovereignty assessment. A green cell marks a subject on which Annex II states a criterion, with the lowest Union assurance level at which that criterion forces SEAL's top answer. Amber marks a subject on which Annex III asks for audit evidence while Annex II states no criterion. Red marks a subject no annex reaches. Grey marks a question whose answers all score SEAL-4, which cannot lower a SEAL level. Weights are the objective weights in the Global Sovereignty Score; within an objective every question has the same weight.

Counted out of the 39 questions that can lower a SEAL level: 14 are reached by an Annex II criterion, 7 of those only partly; 8 appear as Annex III evidence with no criterion behind them; 17 are reached nowhere. Table 3 splits that count by objective.

Objective	Weight	Annex II	Annex III only	Nowhere
SOV-1 Strategic	0.20	1	1	1
SOV-2 Legal and jurisdictional	0.10	4	0	1
SOV-3 Data and AI	0.10	1	1	3
SOV-4 Operational	0.15	4	0	2
SOV-5 Supply chain	0.10	0	4	2
SOV-6 Technology	0.15	0	2	3
SOV-7 Security and compliance	0.15	4	0	2
SOV-8 Environmental	0.05	0	0	3

Table 3. Coverage by objective, counting only the questions that can lower a SEAL level. Weights as the calculator applies them; the framework document (v1.2.1) prints 0.15 for strategic, 0.20 for supply chain and 0.10 for security and compliance, so the Commission's two texts disagree on three of the eight weights.

The coverage concentrates. The Regulation is strongest exactly where the debate has been loudest, on jurisdiction, control, personnel and location. Three objectives have no criterion: supply chain, where Annex III collects the evidence and Annex II states no test; technology openness, where two of five questions reach Annex III and three reach nothing; and sustainability, which neither annex mentions. Those three account for 0.30 of the framework's score between them.

Table 4 is the full crosswalk, one row per question. Provisions are cited by their Annex II paragraph number (2.1(g)(ii) is criterion (g), sub-point ii, at level 2) or by their Annex III audit criterion letter (III I(2)(b) is audit criterion I, evidence item 2(b)).

SEAL question	Reached at	The provision, and its limits
SOV-1.1 EU/EEA legal entity control	**level 4**	3.1(g) prohibits third-country control subject to the Art. 18 route; 4.1(g) absolutely
SOV-1.2 Change of control risk	n/a, score only	no forward-looking ownership test in either annex
SOV-1.3 Control over roadmap	nowhere	no counterpart
SOV-1.4 Financial independence	n/a, score only	Art. 32(3) scores it outside the framework
SOV-1.5 EU economic contribution	n/a, score only	Art. 32(3)(a), non-decisive by Art. 32(2)(d)
SOV-1.6 EU strategic programmes	n/a, score only	no counterpart
SOV-1.7 Industrial strategy alignment	n/a, score only	no counterpart
SOV-1.8 Resilience to cut-off	Annex III only	III I(3)(b),(c): alternative identified, tests, switchover plan; II 2.1(i)(ii) asks only for a plan
SOV-2.1 Primary legal jurisdiction	**level 2**	2.1(a) provider and subcontractors established in the Union
SOV-2.2 Extraterritorial laws	**level 4**	4.1(g) with 4.1(k) separation; 2.1(g) mitigation scores SEAL-2
SOV-2.3 Data access pathways	**level 2**	2.1(g)(ii) access by a third country is prevented

SEAL question	Reached at	The provision, and its limits
SOV-2.4 Export control restrictions	**level 2***	2.1(g)(iv) covers compelled compliance; the exposure of the offer is untouched
SOV-2.5 Origin of IP	n/a, score only	no counterpart
SOV-2.6 IP holder jurisdiction	nowhere	no counterpart; the question floors at SEAL-3
SOV-3.1 Customer control of encryption keys	nowhere	no key-control criterion in either annex
SOV-3.2 Data flows and access logs	Annex III only	III C(1),(4): access logs, privileged access records, data flow diagram, to the auditor
SOV-3.3 Secure deletion and proof of erasure	nowhere	deletion appears once in III C(4), as a flow the diagram must show
SOV-3.4 Data location strictly EU	**level 2***	2.1(c), subject to the buyer's override, which is the SEAL-1 answer
SOV-3.5 AI services under EU control	nowhere	the SEAL-4 answer requires EU chips, out of scope
SOV-4.1 Portability and interoperability	nowhere	no customer-exit criterion; III I(3)(b) is the provider's own switchover
SOV-4.2 Operating without foreign dependencies	**level 3**	3.1(h) support by EU residents, uncontrolled third parties
SOV-4.3 Skill availability	**level 3**	3.1(d) Union citizens, cleared where classified
SOV-4.4 Support channels	**level 3**	3.1(d) with 3.1(h)
SOV-4.5 Documentation and knowledge transfer	nowhere	documentation is not an asset under the Annex III note; the SEAL-4 answer is its answer 3
SOV-4.6 Subcontractor and supplier jurisdiction	**level 2***	2.1(a) subcontractors established in the Union; the calculator's answers here are a copy of SOV-1.8′s
SOV-5.1 Origin of components	nowhere	hardware excluded by the Annex II scope clause
SOV-5.2 Manufacturing location	nowhere	hardware excluded by the Annex II scope clause
SOV-5.3 Firmware provenance	n/a, score only	hardware excluded; SEAL neutralised the question itself
SOV-5.4 Origin of software	Annex III only	III I(2)(b), near-verbatim
SOV-5.5 Software packaging and updates	Annex III only	III I(2)(b), near-verbatim
SOV-5.6 Single point of dependency	Annex III only	III I(2)(c), verbatim
SOV-5.7 Supply chain transparency	Annex III only	III I(2)(e), narrowed to software manufacturers
SOV-6.1 Interoperability and open interfaces	nowhere	no counterpart
SOV-6.2 Open standards compliance	Annex III only	III I(3)(d) asks for the list; Annex II states no criterion

SEAL question	Reached at	The provision, and its limits
SOV-6.3 Open source availability	nowhere	no counterpart; II (j) imposes a duty on open-source use at every audited level
SOV-6.4 Service architecture transparency	Annex III only	III C(4), I(2)(a) to the auditor; nothing published
SOV-6.5 High-performance computing sovereignty	nowhere	hardware excluded by the Annex II scope clause
SOV-7.1 Security certification	**level 4***	4.1(e) requires a European cybersecurity certificate at 'high'; SEAL scores Common Criteria EALs
SOV-7.2 EU regulatory compliance	n/a, score only	GDPR, NIS2 and DORA bind independently
SOV-7.3 EU-based security operations centre, incident handling	**level 3***	3.1(h); SEAL-4 adds ENISA participation
SOV-7.4 Control over monitoring and logging	nowhere	no customer-side logging criterion
SOV-7.5 Disclosure of incidents	nowhere	NIS2 binds separately; Annex II states no criterion
SOV-7.6 Maintenance autonomy	**level 2***	2.1(i)(ii) blocks remote features; patch autonomy is not required
SOV-7.7 Auditability	**level 2***	Art. 20 gives one accredited auditor; SEAL-4 asks for any independent entity
SOV-8.1 Energy efficiency	nowhere	Annex I sets a 1.15 power usage effectiveness (PUE) programme target; no criterion
SOV-8.2 Hardware reuse and recycling	nowhere	no counterpart
SOV-8.3 Environmental impact reporting	nowhere	no counterpart
SOV-8.4 Energy supplies	n/a, score only	no counterpart

Table 4. The crosswalk. An asterisk marks a criterion that covers part of what the question asks; the reason is in the third column. "n/a, score only" marks a question all of whose answers score SEAL-4, which therefore cannot lower a SEAL level, so the comparison does not arise.

5. Five services, scored both ways

Each profile below is constructed from the criteria. None describes a firm. Each placement names the answers that produce it.

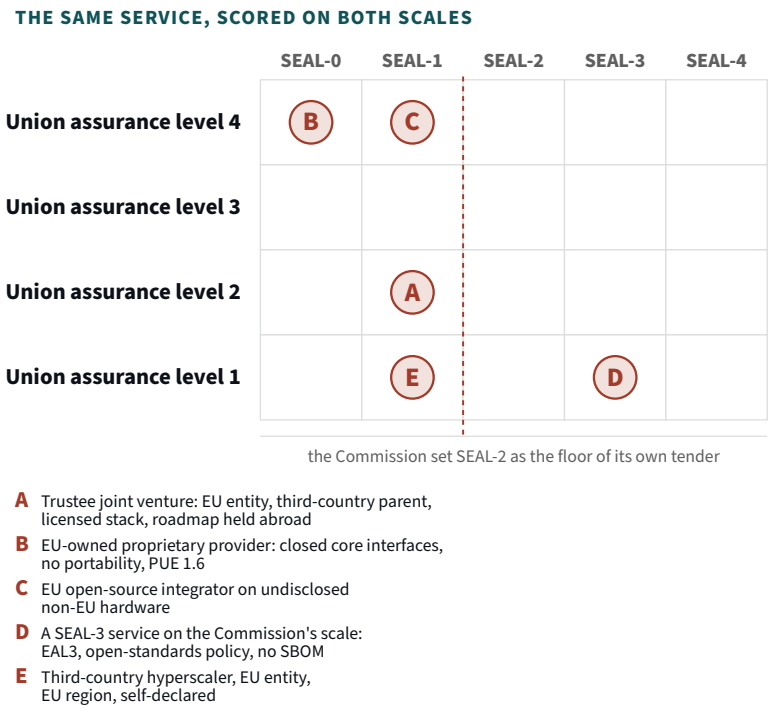


Figure 3. Five profiles on both scales. The dashed line is the SEAL-2 floor the Commission set for its own tender. Nothing lies on a diagonal: the relation between the two scales is not monotone in either direction.

A. The trustee joint venture. Union assurance level 2, SEAL-1. A company established in the Union, operating under a licence from a third-country parent that holds the roadmap, with data, infrastructure and support in the Union, an SBOM, and documented legal, technical and organisational measures neutralising the parent's control. Annex II 2.1(g) is written for exactly this structure. Annex III adds a note under audit criterion I stating that joint ventures of a Union entity with a third-country entity "can qualify for this level". On the framework's scale the same service answers SOV-1.1 at "mostly outside the EU" (SEAL-1), SOV-1.3 at "no influence possible" or "voice of the customer channels" (SEAL-2), and SOV-6.3 at "fully closed-source, vendor-controlled governance" (SEAL-2). The minimum is SEAL-1. Article 30(3) admits this service for public-order workloads in the NIS2 sectors [7], in national security, defence, justice and law enforcement. The Commission's own tender would have excluded it at the floor.

B. The European proprietary provider. Union assurance level 4, SEAL-0. Wholly Union-owned and Union-operated, no third-country control, Union citizens with clearances, a certificate at 'high', a documented effective-control position on every software component. It sells a closed-source platform whose core services use proprietary interfaces and formats, offers no portability guarantee, and runs at a PUE of 1.6. SOV-6.2 scores SEAL-0, SOV-6.1 SEAL-0, SOV-4.1 SEAL-1, SOV-8.1 SEAL-1. The service sits at the top of one scale and the bottom of the other. The profile describes a normal European enterprise software business.

C. The European open-source integrator. Union assurance level 4, SEAL-1. Union-owned, a fully open-source stack under Union-based governance, customer-held keys, open standards throughout, Union staff. Its servers are designed and fabricated outside the Union and it discloses nothing about their provenance, because no one has asked. The Annex II scope clause puts hardware outside the criteria, so nothing stops level 4, subject to (e), which where no scheme yet applies is satisfied by demonstrating compliance with the highest cybersecurity standards under Union law. On the framework, SOV-5.1 answers "no disclosure" (SEAL-1) and SOV-5.2 "fully foreign, black box" (SEAL-1). Profiles B and C hold the same Union assurance

level, sit one band apart on SEAL, and differ for opposite reasons. The Union assurance level says nothing about either difference.

D. A service at SEAL-3. Union assurance level 1 at most. Union-controlled, Union law, a formal open-standards policy for most core services, open source with centralised governance, Union teams, most suppliers auditable, Common Criteria EAL3, customer-controlled logs stored in the Union, PUE 1.3. This is a strong offer on the Commission's scale and comfortably above the floor it set. Nothing asked it for a software bill of materials, so it has none. Its certificate is a Common Criteria evaluation where Annex II 2.1(e) asks for a European cybersecurity certificate. That criterion and 2.1(i)(i) are therefore both unmet, so level 2 is out of reach until the paperwork is done.

E. The third-country hyperscaler. Union assurance level 1, SEAL-1. An entity established in the Union, infrastructure and customer data in a Union region, support outsourced outside the Union under contractual safeguards, subcontractors disclosed. Level 1 permits third-country control and screens it on one specific legal feature: whether a law of the controlling country requires the provider to report software vulnerabilities to its authorities before those vulnerabilities are known to be exploited. A provider from a country with no such law passes. Level 1 is self-assessed under Article 19. Article 30(2) makes it the requirement for every public sector activity not identified as contributing to the preservation of public order. On the framework, SOV-2.3 answers that non-EU authorities can compel access (SEAL-1) and SOV-1.1 that decision authority is outside the Union (SEAL-1).

Profiles A and E are the two that matter politically, because between them Article 30(2) and Article 30(3) cover the public sector estate.

6. Where the divergence comes from

6.1 The scope clause

Annex II opens by putting software within the meaning of Article 3(4) of Regulation (EU) 2024/2847 inside its scope and hardware within the meaning of Article 3(5) outside it, for both Annex II and Annex III [3]. The criteria regulate hardware's *location*: criterion (b) requires infrastructure and assets in the Union, evidenced in Annex III by server addresses, lease agreements and asset registers. Its *provenance* goes unregulated. Where a server was designed, where it was fabricated, and whose firmware it runs are questions the Regulation does not ask.

The framework asks all three, at SOV-5.1, SOV-5.2 and SOV-5.3, and cannot answer them either: its own lessons-learnt section reports that SEAL-4 "is not today relevant in the context of EU Sovereignty considering existing dependence to specific supply chains (chips, hardware)", and proposes relaxing the level so that it discriminates between providers again. SEAL neutralised SOV-5.3 in the calculator itself, by giving every answer to the firmware question a SEAL-4 value.

So both instruments arrive at the same wall and take opposite routes. The framework keeps the question and makes the top level unreachable. The Regulation removes the question and makes the top level reachable. The second route has a cost the first does not. A buyer reading "Union assurance level 4" learns nothing about hardware provenance. Nothing on the label records that the question was left out.

Hardware then reappears in Article 32(3)(d), which lets contracting authorities evaluate whether the service is delivered through "critical computing, storage and networking hardware components designed and/or manufactured in the Union", or where that is not feasible through third-country components contributing to security of supply. Article 32(2)(d) requires that criterion, along with every other non-price criterion, to be "ancillary and not decisive in the award of the contract".

6.2 Openness: an asset in one instrument, a liability in the other

The framework treats openness as a component of sovereignty and scores it four ways: open interfaces (SOV-6.1), open standards (SOV-6.2), open source with the right to audit, modify, redistribute and transfer stewardship (SOV-6.3), and architecture transparency (SOV-6.4). Together these weigh 0.12 of the Global Sovereignty Score and any of the first two can cap a service at SEAL-0.

The Regulation mentions open source once, at criterion (j). It is a duty. Where software released under an open-source licence is used, the provider must implement and document controls preventing remote features that could tamper with or disrupt a device, system or software. The parallel duty on proprietary components, at (i)(ii), bites only when they are provided, owned and licensed by a third-country entity. The burden therefore falls on the class of component whose source can be read, and lands on European assemblers. A European proprietary vendor bears no duty of either kind.

Annex III shows that the drafters knew what the missing criterion looks like. Audit criterion I(3)(d) asks the provider to "provide a list of open standards that are followed as part of the audited providers policies regarding the audited service". Nothing in Annex II says what must be on that list.

6.3 The exit channel

Annex II contains no portability or interoperability criterion. Annex III I(3)(b) and (c) require the provider to identify alternative software solutions, implement tests and hold a switchover plan. The beneficiary there is the provider's own continuity against a failing vendor. Nothing in either annex is owed to a buyer who wants to leave.

The framework's bar is low and it exists: SOV-4.1 awards SEAL-4 from its third answer, "standard documented methods for data export are available", which Chapter VI of the Data Act already requires of every provider in the Union [4]. A criterion that restates law in force costs a compliant provider nothing and gives the auditor something to test. An incumbent's markup over the alternative is bounded by what leaving would cost the buyer. Across European cloud and software fewer than one per cent of customers switch provider in a year [8]. A framework that screens a supplier's jurisdiction and says nothing about its exit cost certifies the channel that gets discussed and leaves the channel that operates continuously.

6.4 Control: defined and binary, or graded and undefined

The Regulation defines control by reference to Article 2(6) of Regulation (EU) 2021/697 [6], the ability to exercise a decisive influence directly or through intermediate legal entities. It then uses the definition as a switch: permitted at level 1, mitigable at level 2, prohibited at levels 3 and 4. The framework grades it, from "entirely outside the EU" to "entirely within the EU" across five answers, and defines none of them.

Each failure mode is the other's strength. A binary test defined on decisive influence is auditable and can be engineered around, through stakes below the threshold, veto rights, board nomination rights or commercial and financial dependence. A graded test captures partial influence and leaves the evaluator with no anchor for "mostly".

Annex III already resolves this better than either. Audit criterion G requires the auditor to identify every direct and indirect shareholder up to the ultimate owners, together with the cap table behind them. It then requires the bodies empowered to take strategic decisions, the rules for appointing and removing them, the quorums and majorities those decisions need including blocking rights, and any influence running through commercial or financial links. Its disclosure threshold is 5% of capital or voting rights, with a list of veto, pre-emption and conditional purchase rights. That is the operational definition both instruments need. It currently sits in an evidence list.

7. What Annex III already borrowed

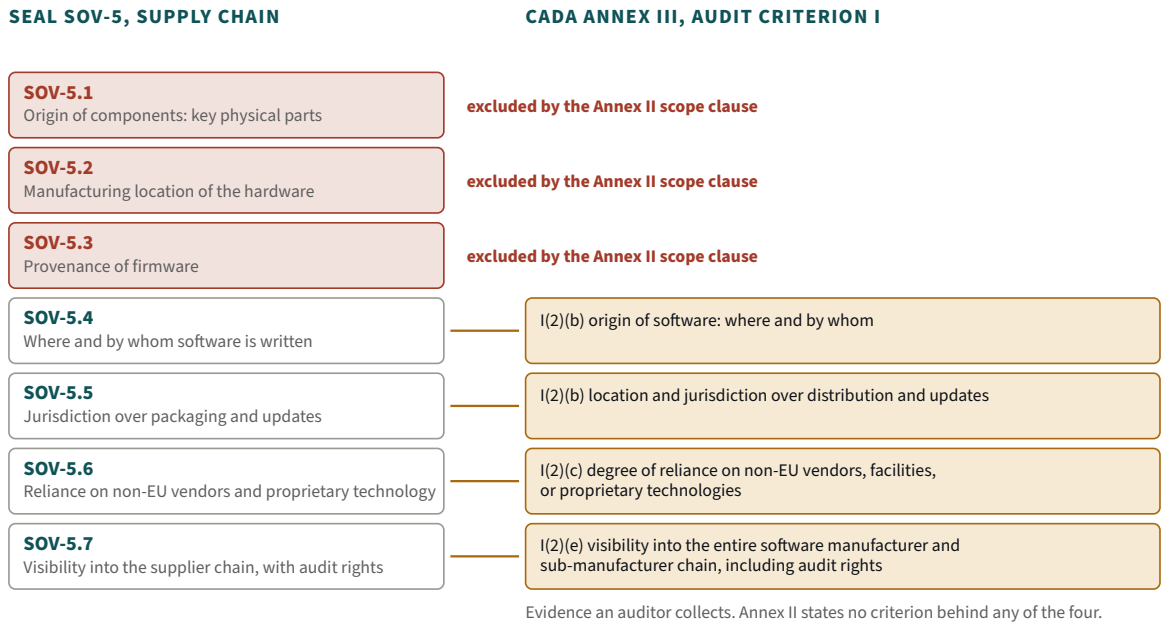


Figure 4. SEAL's supply-chain objective and audit criterion I of Annex III. Four of the seven questions are restated in the Regulation's evidence list, near-verbatim, narrowed from suppliers and sub-suppliers to software manufacturers and sub-manufacturers. The three the scope clause removes are the three about hardware, one of which (SOV-5.3, firmware) the framework had already neutralised in its own calculator.

The correspondence is close enough to read as a lift. Annex III asks the audited provider to disclose "origin of software: where (country of origin) and by whom the software is designed, developed and maintained, the location and jurisdiction governing the software distribution, and updates" (I(2)(b)), which is SOV-5.4 and SOV-5.5 joined; "degree of reliance on non-EU vendors, facilities, or proprietary technologies" (I(2)(c)), which is SOV-5.6 word for word; and "visibility into the entire software manufacturer and sub-manufacturer chain, including audit rights" (I(2)(e)), which is SOV-5.7 with "supplier and sub-supplier" replaced.

None of the four has a criterion behind it in Annex II. An auditor collects the disclosure, records it in the audit report, and has nothing to test it against. Criterion (i) at levels 2 and 3 requires an SBOM, tamper controls, source-code audits of security-relevant third-country components and a migration plan, and says nothing about the degree of reliance the disclosure reveals. At level 4 the effective-control test of 4.1(i)(ii) does bite. It is the one provision in the Annex that asks who can change a component over time.

8. What the co-legislators should do

These are ranked by consequence. Each names its vehicle.

1. Promote Annex III's imported supply-chain lines into Annex II. Three items go into criterion (i) at level 3, covering the four SEAL questions, because I(2)(b) holds two of them:

- the origin of software, as Annex III I(2)(b) defines it;
- a stated and assessed degree of reliance on non-EU vendors, facilities and proprietary technologies, as in I(2)(c);

- visibility into the supplier and sub-supplier chain with audit rights, as in I(2)(e), restoring the wider scope the framework uses.

I(2)(c) already contains a level-3 clause on licensing restrictions, which the promotion should keep in place.

This is the cheapest amendment in this note. The text exists and was drafted by the same hand. Promotion converts evidence an auditor merely collects into a criterion a service can fail.

2. Extend the effective-control test of 4.1(i)(ii) down to level 3, and state what it costs to exercise the alternative. Level 4′s test asks whether a third country or third-country entity can materially influence the technical evolution, maintenance priorities, security remediation and long-term continuity of a component. It is the only provision in Annex II that measures the property determining whether a European buyer has an option at all. Where a component's upstream is under third-country control, the migration plan the Annex already requires should name the alternative and state what exercising it would cost.

3. Add an exit criterion, at level 2 and above. Criterion (l): documented, standard, tested methods for the customer to export data and workloads, with the switchover evidence already drafted at Annex III I(3)(b) extended from the provider's own change of vendor to the customer's. It restates Chapter VI of the Data Act inside the instrument that certifies the supplier, where an auditor can test it. It creates no obligation that Union law does not already impose.

4. Decide what the label says about hardware. Delete the scope exclusion and add a disclosure criterion at level 2: component origin, manufacturing location and firmware provenance disclosed, with no Union-origin requirement. That costs a provider nothing it does not already know, and gives the Union data it presently lacks. Or keep the exclusion and say so in Article 16(1), so that a buyer reading a Union assurance level knows what was not assessed. The first is better. The second is the minimum.

5. Move the data-residency override out of Annex II and into Article 30. Delete "unless the public sector body explicitly requires otherwise" from 1.1(b), 1.1(c), 2.1(c) and 3.1(c). Recognition under Article 17 is Union-wide and per service; a waiver is per contract and per buyer. If the waiver is wanted, it belongs in Article 30(4) alongside the other derogations, where it must be justified and can be published.

6. Add the openness criteria, and make criterion (j) origin-neutral. Annex III I(3)(d) already asks for the list of open standards. Annex II should say what has to be on it for core services, and should score open interfaces the way SOV-6.1 and SOV-6.2 do. On (j), fold the open-source duty into (i)(ii) so that the tamper-control obligation attaches to the component's control structure rather than to its licence.

7. Fix three drafting points in the annexes.

- Annex II 3.1(g) refers to "an implementing act under Article 19". Article 19 is conformity self-assessment and confers no implementing power. Article 18, associated third countries, confers exactly this power: under Article 18(1) the Commission "may adopt decisions, by means of implementing acts, identifying third countries for which cloud computing service providers subject to the control of that third country … may be audited against the criteria for Union assurance level 3", which is the route 3.1(g) opens. Correct the cross-reference, and take the separate decision about whether the route should exist on its merits; the two sister CADA positions take that decision and ask for its deletion, and this note asks only that the text say what it means.
- The note under Annex III audit criterion I, stating that joint ventures of a Union entity with a third-country entity "can qualify for this level", settles a question of who qualifies inside an evidence list. Move it to Annex II or delete it.

- Annex II 4.1(c) narrows data residency to data a risk assessment identifies as sensitive. Read with Article 20(1) the lower levels' criteria still apply, so the narrowing has no effect, which the drafters cannot have intended. Align the wording.

8. Publish both measures for every recognised service. Article 22 establishes a central repository of recognised services and is the vehicle. An entry giving the Union assurance level and the framework's eight objective scores would show the divergence to buyers, to the Parliament and to suppliers deciding what to invest in. It costs one column. Article 15 monitors the compute capacity gap and is not the place for it.

What the Commission can do under the current text. The framework is due a revision. Four points should go into it. SOV-4.6′s answer set in the published calculator is a copy of SOV-1.8′s and does not answer the question the row asks. Nine of the 48 questions have the same SEAL value on every answer, which makes them score-only; where that is deliberate it should be stated per question, as the guidance states it in general. The minimum rule also lets a question weighted at 0.0125 of the score cap the entire assessment: a PUE above 1.5 forces SEAL-1 whatever else is true. Either the environmental objective sits outside the minimum, or its thresholds move. Aligning SOV-7.1 onto the Regulation's certification scale would also remove the one place where the two instruments measure the same property and cannot be compared.

9. Asks already on the table

Each is argued at length in positions on this file that are not yet published.

- Article 30(3) to read "level 3 or 4" in place of "level 2, 3 or 4".
- The disproportionate-cost derogation in Article 30(4), which the Commission text letters (a) a second time, to be defined, computed on lifecycle cost including exit cost, and published.
- Article 16(2), the delegated power over Annexes II and III, to include a non-regression clause.
- Article 32(2)(d) to be deleted, so that a non-price criterion can decide an award.
- Article 38(5), central purchasing, to bind the strategic direction of each procedure to the Article 30 assurance levels.
- Article 41 to require what it currently encourages.

Annex A: how the crosswalk was coded

The coding rule of the About section leaves a small number of judgement calls. Each is set out below.

Partial coverage. Seven rows have an asterisk. SOV-2.4: 2.1(g)(iv) forbids a controlled provider from being compelled to apply foreign restrictive measures, while the framework's top answer requires that part of the offer cannot be exposed to such measures at all, which reaches inputs the Annex II scope clause excludes. SOV-3.4: the criterion is defeated by the buyer's override, which is the framework's answer 4 and scores SEAL-1. SOV-4.6: 2.1(a) covers where subcontractors are established, while the question also asks about their legal control. The calculator's answer set for this row is separately defective: its five answers are a copy of SOV-1.8′s and do not answer the question the row asks. SOV-7.1: the two instruments use different certification scales. SOV-7.3: the criterion covers support and incident handling location, while the top answer adds participation in ENISA information-sharing. SOV-7.6: the criterion blocks remote tamper features, while the question asks about the customer's autonomy to schedule and test patches. SOV-7.7: Article 20 provides one accredited auditor of conformity, while the question asks for full audit access by any independent entity.

Level attribution. Where a criterion appears at several levels in different strengths, the row gives the lowest level at which the criterion excludes every answer below SEAL-4. SOV-1.1 is coded at level 4 because 3.1(g) admits a derogation, under which a service recognised at level 3 is still subject to third-country control. SOV-2.1 is coded at level 2 because level 1 requires establishment of the provider alone.

Two rows that could be read the other way. SOV-3.2 is coded Annex III only, because the access logs and privileged-access records of audit criterion C run to the auditor, while the question asks about the customer's real-time visibility. SOV-6.4 is coded the same way and for the same reason. A reader who treats disclosure to an auditor as equivalent to disclosure to the customer would move both to Annex II, which would change the count of section 4 from 14 to 16 and leave every other finding intact.

Which 48 questions. The implementation guidance describes an assessment "composed of 43 questions"; the published calculator holds 48. This note counts the calculator, the artefact that computes a level. Every SEAL value and weight quoted here is read from it, the guidance's own tables being screenshots.

What is not coded. The comparison runs between Annex II, Annex III and the framework's 48 questions. Obligations that reach a cloud service from elsewhere in Union law, chiefly the GDPR, NIS2, DORA and Chapter VI of the Data Act, are noted in the third column where relevant. They are not counted as coverage: they bind whether or not a service seeks recognition, and do not vary by assurance level.

References

1. European Commission, *Proposal for a Regulation establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act)*, COM(2026) 502 final, 3 June 2026, with Annexes I to III. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52026PC0502
2. European Commission, *Cloud Sovereignty Framework: Implementation guidance*, Cloud III Dynamic Purchasing System, with the annexed sovereignty assessment calculator. The framework itself is version 1.2.1, DG Digital Services, 20 October 2025. https://commission.europa.eu/document/download/2ad80a48-166f-4c77-a513-80c53ca2a128_en
3. Regulation (EU) 2024/2847 (Cyber Resilience Act), Article 3, points (4), (5), (6), (13) and (39). http://data.europa.eu/eli/reg/2024/2847/oj
4. Regulation (EU) 2023/2854 (Data Act), Chapter VI on switching between data processing services. http://data.europa.eu/eli/reg/2023/2854/oj
5. Regulation (EU) 2019/881 (Cybersecurity Act), on European cybersecurity certification schemes. http://data.europa.eu/eli/reg/2019/881/oj
6. Regulation (EU) 2021/697 (European Defence Fund), Article 2, points (6), (21) and (22), for the definitions of control, classified information and sensitive information that CADA imports. The description of control in section 6.4 paraphrases point (6) and does not quote it. http://data.europa.eu/eli/reg/2021/697/oj
7. Directive (EU) 2022/2555 (NIS2), Annexes I and II, for the sectoral perimeter of Article 30(3). http://data.europa.eu/eli/dir/2022/2555/oj
8. Fermigier, S. (2026a). *Exit, Pursued by a Bill: Lock-in Rents and Portability in European Cloud and Software.* Draft working paper v0.14, 2026-09-23. Abilian Econ Lab. https://econ.lab.abilian.com/papers/rent-channel/