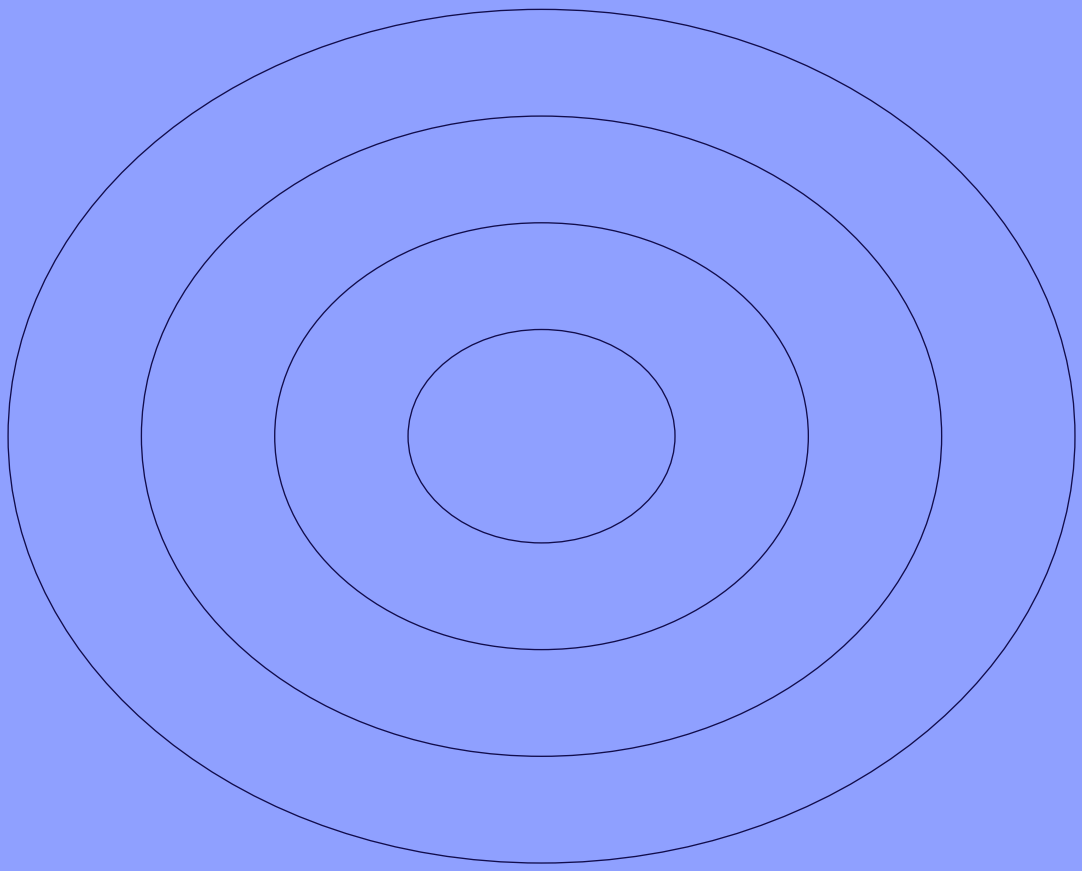
FOTI



Strengthening the EU's Cloud & AI Development Act

# Step 1: Map the Risk

## How to better understand our dependencies

A report series by FOTI
November 2026

FOTI

## About FOTI

FOTI is a European think tank dedicated to building a prosperous and fair future that harnesses the power of technology.

We help democracies tackle some of the biggest technology challenges of our time. From market concentration and digital sovereignty to platform accountability and industrial policy, we develop practical solutions that strengthen innovation, support challengers and deliver better outcomes for people and societies.

## About this series

*Strengthening the EU's Cloud & AI Development Act* is a report series by FOTI.

**Step 1: Map the Risk: How to better understand our dependencies**
Strengthening the EU's Cloud & AI Development Act
November 2026

# Table of contents


01 Executive summary 04

02 Context:
*You can't solve a dependency you don't track* 05

- What we know about our dependencies 06
- How dependencies are assessed today 07
- What CADA does to address this 08

03 CADA's weakness:
*Dependencies will remain unclear* 10

04 Our proposed fixes 12

- A. Reporting and monitoring obligations of Member States and the Union 13
- B. Private sector assessment of dependencies 19

Sources and resources 23

# 01 / Executive summary

Europe knows it depends on foreign cloud, but it doesn't know how or where. Aside from the well-known headline – three hyperscalers control over 70% of Europe's cloud market – no published source measures the market by detailed ownership or supply chain control.

Part of the problem is that public buyers do not track their reliance on foreign cloud in any standardised, centralised way. In the Netherlands, for example, ministries could not name the source of a quarter of their 1,588 cloud services and had assessed the risks of just a third of services used for key government functions.

CADA creates the right instruments (e.g., national strategies, capacity monitoring, public sector risk assessments, impact assessment for private operators, procurement reporting), and we support them.

**But – as drafted – these instruments will not produce a reliable, current and shared picture.** *What* is measured is undefined, reporting is sporadic, results are not public, and private industries that run critical infrastructure are not required to track.

We recommend continuous monitoring of public cloud procurement held in a public register (A.1); publication by default (A.2); protection for whistleblowers (A.3); mandatory dependency assessments for private operators of services covered by NIS2 (B.1); and a right for those operators to obtain supply chain information from their providers (B.2).

# 02 / Context:

*You can't solve a dependency you don't track*

Reducing a dependency starts with measuring it. This section sets out what Europe knows about its cloud and AI dependencies, what it does not know, how those dependencies are assessed today, and what the proposal does about it.


## What we know about our dependencies

Page 6

## How dependencies are assessed today

Page 7

## What CADA does to address this

Page 8

# What we know about our dependencies

**The market is concentrated, and the concentration is stable.** European cloud providers' share of the European cloud infrastructure market fell from 29% in 2017 to 15% in 2022 and has held at about 15% since. Amazon, Microsoft and Google together hold about 70%; the largest European providers, SAP and Deutsche Telekom, hold 2% each.

But European providers are not shrinking: at the time of the latest published figures the market was growing at around 24% a year, and their revenues grew with it. A constant share of a fast-growing market means the gap in absolute euros widens every year while the ratio holds. The accurate description is revenue growth without share growth.

**The dependency runs below the service, into the hardware stack.**
The services Europe buys run on hardware and software that Europe does not make. The Commission's impact assessment for the Chips Act 2.0 proposal estimates that "96% of the semiconductor market for data centres is captured by US-owned companies" and concludes that the Union's AI infrastructure and software "will potentially be structurally dependent on extraterritorial US jurisdiction and policy choices". The Communication presenting the Technology Sovereignty Package records that the Union produces "only around 10% of global semiconductors" and remains "excessively reliant on non-EU suppliers" for "the supply of key components of advanced digital infrastructure including semiconductors, cloud computing and essential AI hardware and solutions". New capacity, too, is mostly built by others: "the ongoing expansion of data centre capacity in the EU is driven by non-European cloud services providers" (CSPs), and the three largest providers are expected to "drive 65% of the demand for DCs in Europe by 2028".

**At the software layer, a "sovereign" label can hide a dependency.** The impact assessment records that Delos Cloud, an SAP subsidiary operating on Microsoft software for German public administrations, "is deemed by the Interior Ministry of the State of Baden-Württemberg to not be fully sovereign beyond its infrastructure", because the application layer "remains subject to the requirements of the US CLOUD Act, giving rise to data access without the customer's awareness". Where a dependency sits, whether it is in the data centre, in the operator, in the software licence, or in the chip, determines who can act on it. That is why any meaningful evaluation must cover the whole stack, from software to individual hardware components.

**The exposure this creates is legal and technical, not only commercial.**

Under the US CLOUD Act, a provider within US jurisdiction must preserve and disclose data within its "possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States". The reach attaches to control of technology and data access, not to location: an EU-registered subsidiary whose parent can obtain the data is within it. An assessment of dependencies must therefore be legal as well as technical, and it cannot be a one-off.

# How dependencies are assessed today

The headline figures are widely known, but not well understood.
Four gaps matter for any evaluation of sovereignty:

**No published source measures the European market by technology control.** Five sources are in circulation. They measure five different things, and only one of them says anything about who the provider is.

## Five sources, five measures of the European market

| Source | "European" definition | What it measures | Result |
|---|---|---|---|
| Synergy Research Group | Provider headquarters | Revenue from IaaS, PaaS and hosted private cloud | European providers hold 15% of the European market |
| Eurostat, ICT usage survey | N/A (Provider nationality is not a variable in the survey) | Share of enterprises buying cloud services | 52.7% of EU enterprises in 2025 |
| Commission impact assessment, capacity section | Physical location of the infrastructure, whoever owns it | Installed computing capacity | The EU hosts 20% of global capacity |
| CBRE | Geography of the asset (includes the UK, Norway and Switzerland) | Live and pipeline megawatts | 13 GW by end-2026, of which hyperscaler self-built 4.3 GW |
| Gartner | A service attribute and buyer intent (e.g. non-EU headquartered providers' "sovereign" offerings count) | Spend on services marketed as sovereign | Europe: $6.9 billion (2025) to $23.1 billion (2027) |

A capacity-based measure makes Europe look better and is the one incumbents prefer; a headquarters-based measure makes Europe look worse and is the one European providers prefer. Neither answers who can be compelled by a foreign authority to change the terms of a service. Nobody publishes that measure.

**Public buyers lack visibility into their cloud usage and risks.** In 2025, the Netherlands Court of Audit revealed that ministries could not classify 26% of their 1,588 cloud services between public, private, and hybrid cloud, skipped risk assessments for 67% of critical services, and heavily depended on U.S. tech giants due to limited internal expertise . Similarly, a French audit in 2025 found fragmented strategies, underused sovereign

platforms despite €55 million invested, and unmanaged foreign dependencies. As the only two published national audits of their kind, these findings likely reflect a broader trend across other EU Member States and institutions.

**In the private sector, only financial services track dependency.** Under the Digital Operational Resilience Act, every financial entity must maintain and update a register of information on all its contractual arrangements with ICT third-party providers, report on it yearly to its competent authority and make the full register available on request. On 18 November 2025 the three European Supervisory Authorities used those registers – "the ESAs collected data from the Registers of Information maintained by financial entities" – to designate the first critical ICT third-party providers subject to Union oversight. It is the only continuously maintained, legally mandated map of cloud dependencies in the Union, and it exists because the sector was required to build it. Outside finance, essential entities under the NIS2 Directive must address "supply chain security" in their risk-management measures, but nothing requires them to record, report or assess their dependency on any provider.

**The EU calls for tracking and assessing dependency, but does not publish its own.** The Communication presenting the package states that the Union's vision for technological sovereignty "must be grounded in a clear assessment of its critical technological dependencies". The Communication states that "an initial assessment of dependencies has been carried out" in the field of open source, and notes that the software bills of materials generated under the Cyber Resilience Act, "even if these are not published", can be used by market surveillance authorities with ENISA "to perform an EU-wide dependency assessment". To our knowledge none of these assessments has been published, and none of them reaches a customer who has to decide what to buy.

**The Commission timidly started assessing sovereignty for itself.** For its own purchases the Commission has built a Cloud Sovereignty Framework: 48 criteria in eight categories, from legal and jurisdictional exposure to supply chain and technological autonomy, scored into Sovereignty Effectiveness Assurance Levels (SEAL). It used the framework to award, in April 2026, a EUR 180 million contract for sovereign cloud services to Union institutions, bodies and agencies, and it "encourages all organisations, both public and private, to consult and use this framework".

**What CADA Does To Address This**

The proposal creates a series of assessments, reports and monitoring requirements throughout the text, from national strategies to capacity monitoring and dependency assessments. Each plays a specific role in building a thriving cloud and AI industry.

**Article 7 requires Member States to "establish national cloud and AI strategies".** The strategies must contain "at least" objectives and priorities for cloud and AI adoption, a governance and monitoring framework, measures on adoption by public bodies and SMEs, data centre capacity, computing infrastructure, public procurement of cloud and AI, open cloud stack technologies and access to data for AI. They are notified to the Commission and reassessed at least every three years against key performance indicators. The Commission's role is to monitor; the European Artificial Intelligence Board may coordinate Member States and facilitate the exchange of best practices (Article 7(6)).

**Article 15 requires the Commission to "identify and monitor"** the compute capacity available in the Union, including edge capacity; the volume of demand for data centre capacity; and "the size of the capacity gap and underserved areas", which may be identified in cooperation with Member States and used as acceleration zones. The monitoring feeds two other provisions: the designation of acceleration zones, and the strategic project criterion in Article 14 for areas identified as having a shortage. The article sets no frequency, methodology or data source, and requires no report or publication.

**Article 29 requires Member States and Union entities to carry out risk assessments.** The assessments must identify the public sector activities using cloud services that "contribute to the preservation of public order" in the sectors listed in the NIS2 Directive, and determine which Union assurance level (2, 3 or 4) is appropriate for each activity, considering:

- the sensitivity, criticality and magnitude of the data;
- the risk of unlawful third-country access and the risk of service disruption;
- whether a multi-vendor or multi-cloud strategy is appropriate.

The Commission specifies the methodology and templates by implementing act and may, where it concludes that the level chosen "is not appropriate or does not adequately address the public order concerns", specify the Union assurance level needed for the sector. Assessments are carried out every two years "or whenever necessary", and Member States send the results to the Commission within three months.

**Article 31 allows private entities in the sectors of high criticality (Annex I of the NIS2 Directive) to carry out assessments similar to those in Article 29.** The exercise is voluntary, and the article does not say whether the results are shared with national authorities or the Commission. Paragraphs 2 and 3 allow the Commission to "issue guidance" on methodology and mitigation measures and, where duly justified, to adopt delegated acts requiring an assessment and mitigation measures from entities in specific circumstances. In other words, private operators are not required to assess or mitigate their dependencies unless the Commission identifies a reason to require it.

**Article 33 requires Member States to "monitor and report on their use of procurement of innovation in cloud computing services and AI systems".** Each year they inform the Commission of the size of the participating economic operators; SME participation trends, including contracts awarded, share of contract value and, "where available", cross-border participation; and the measures taken to improve SME access. The article also sets an objective of 25% of procurement for cloud computing services and AI systems awarded to innovative SMEs, and asks contracting authorities to promote preliminary market consultations, matchmaking with European SMEs and start-ups, and SME-friendly contract clauses.

# 03 / CADA's weakness:

## *Dependencies will remain unclear*

Strategies, risk assessments and monitoring are the right instruments, and their inclusion in the text is welcome. As they stand, however, they are unlikely to give policymakers, public buyers or the market a reliable and up-to-date picture of Europe's cloud and AI dependencies, or to empower and protect those who could report misuse and third-country interference in digital supply chains.

**Gaps in CADA**

01

### Too many terms are left undefined.

Several obligations rest on notions the text does not specify. National strategies are assessed against key performance indicators that the text leaves to each Member State. The capacity gap is to be monitored without a stated methodology, frequency or output, and without any sovereignty dimension. The objective of awarding 25% of cloud and AI procurement to "innovative SMEs" is not defined. The methodology for public sector risk assessments is left to a later implementing act with no deadline (Article 29(3)), while private operators are offered optional guidance (Article 31(2)). Without common data and definitions, Europe can't compare results across Member States and progress will be impossible to show. The Commission's impact assessment identifies the problem well: "users do not have a reliable means of verifying whether a service is truly sovereign or not". Clearer terms and methods address that gap.

02

### Reporting is periodic, while dependencies change continuously.

National strategies are assessed every three years and public sector risk assessments are every two years. This improves on the four years the impact assessment proposed . Reassessment is possible "whenever necessary", but the text does not say what would trigger it. In a market where providers, ownership and contracts can change within months, a public authority's exposure may shift significantly shortly after an assessment and not be spotted until the next cycle. Elsewhere the Union has chosen a better model: in finance, a register is updated as contracts change and reported on every year. CADA's framework risks describing past dependencies – continuous monitoring is more effective.

03

## The information stays between Member States and the Commission, with no transparency.

None of the strategy, assessment and monitoring provisions requires results to be published, even in aggregated form, or reported to an elected institution. The only report to the co-legislators is the general evaluation of the Regulation, four years after its entry into force (Article 47). This limits democratic oversight of a framework justified by public order and national security. It is also a missed opportunity for industry: aggregated information on capacity gaps, public sector demand and required assurance levels would show European providers and investors where the market needs them, and enable the investments the CADA hopes to spark. The Union already publishes this kind of picture for another strategic input: the Critical Raw Materials Act requires the Commission to make available on a free-access website a regularly updated monitoring dashboard of supply risks, built on stress tests carried out at least every three years. For cloud, the proposal's monitoring framework for the purchase of sovereign cloud services in Europe starts from a baseline of zero for the value of sovereign procurement and "NA" for compliance by contracting authorities.

## from mandatory dependency assessments creates a dangerous blind spot.

In sectors like energy, transport, banking, and health, vital services are predominantly run by private firms, and the risk to public order from a cloud disruption is identical regardless of whether an entity is public or private. The Commission originally recognised this in its impact assessment, proposing mandatory assessments for an estimated 25,600 private essential entities under NIS2 Annex I – costed at €1.44 billion in recurrent administrative costs. But by the time CADA came out, this had been significantly diluted. Now, Article 31(1) sets out this assessment as an option.

04

## Exempting critical private operators

# 04 / Our proposed fixes

We make five recommendations, in two groups. The first group strengthens the reporting and monitoring obligations of the Member States and the Union; the second brings private operators of essential services into the picture. For each, we state the problem and the proposed changes, provision by provision.

A. Reporting and monitoring obligations of Member States and the Union


A.1 **Continuous monitoring and a central register of public procurement results** Page 13

A.2 **Transparency obligations for democratic oversight and industry use** Page 15

A.3 **Protection of whistleblowers reporting infringements of the cloud computing sovereignty framework** Page 17


B. Private sector assessment of dependencies


B.1 **Mandatory assessment of dependencies by private operators of essential services** Page 19

B.2 **A right for private operators to obtain supply chain information** Page 21

A. Reporting and monitoring obligations of Member States and the Union

# A.1 Continuous monitoring and a central register of public procurement results

The risk assessments of Article 29 and the private assessments of Article 31 look at what a buyer needs; the procurement obligation of Article 30 and the award criteria of Article 32 decide what it buys. Nothing in the proposal publishes the result. Monitoring exists only for procurement of innovation under Article 33, once a year, on three data points related to SMEs. Whether a contracting authority bought a recognised service, at which assurance level, from which provider, under which procedure and for how much is reported to nobody.

**The needed shift towards sovereign services will be far more effective if it is conducted in public.** That assessment and continuous monitoring would be the feedback loop of the whole Act. It would show where recognised services are being bought and where derogations are used; it would tell national strategies, strategic project designation and the Commission's capacity monitoring where public demand is; and it would tell European providers which sectors and services need them. We suggest that the co-legislators not differentiate, for monitoring purposes, between procurement falling under Article 30 and under Article 32: the results of both should be reported continuously by contracting authorities to a national authority and to the Commission, and held in a central register. An annual reporting channel between Member States and the Commission already exists in Article 33; CADA should widen the scope of those reporting channels to include more than public procurement using the Union Added Value provision, better define the assessment through it and to keep the result in one place.

**Proposed changes:**

01 **Scope of monitoring (Article 33(1)).** Extend the monitoring obligation from procurement of innovation to all procurement of cloud computing services and AI systems by contracting authorities and Union entities, whether under Article 30 or Article 32.

02 **Data points (Article 33(3), new point (d)).** Add, for each contract, the procedure used, the Union assurance level required and the level of the service procured, the provider and whether it or its ultimate parent is established outside the Union, and the contract value – reported as contracts are awarded, not once a year.

03 **Central register (Article 22, new paragraph).** Require the Commission to hold the reported results in the central repository, continuously updated, with a non-confidential aggregate available to the public.

04 **Use of the register (Articles 7(5), 14(1), 15 and 29(2)).** Require national strategies, strategic project designation, capacity-gap monitoring and public sector risk assessments to take the register into account.

A. Reporting and monitoring obligations of Member States and the Union

# A.2 Transparency obligations for democratic oversight and industry use

Title IV of the proposal relies on a series of strategies, assessments and monitoring exercises to build a picture of Europe's cloud and AI dependencies. We support this approach. However, almost none of these provisions requires the resulting documents to be made public, and none anticipates that they could be used by anyone other than the Member States and the Commission. The knowledge the Regulation creates therefore stays with the authorities that produce it. This is a missed opportunity on three counts:

- **Democratic oversight.** The European Parliament and national parliaments cannot scrutinise decisions justified by public order and sovereignty if they cannot see the evidence behind them.
- **Civil society.** Researchers, journalists and civil society organisations cannot react to, challenge or complement the assessments, nor flag dependencies that authorities have missed.
- **Industry.** European providers cannot invest in services for which they see no market. A provider that does not know which sectors need higher assurance levels, where capacity is short, or which components of the cloud stack have no European offer has no signal to build them.

We propose a general principle of **publication by default**, adapted to the sensitivity of each instrument.

**Proposed changes:**

01 **National cloud and AI strategies (Article 7).** Member States should publish their strategies, the key performance indicators they use, and the results of each three-yearly reassessment in full.

02 **Capacity monitoring (Article 15).** The Commission should publish an annual report on available compute capacity, demand, the capacity gap and underserved areas, at a level of geographic detail sufficient to guide investment decisions. This is crucial – at the moment the need to "triple" Europe's compute capacity is asserted, but the basis for the conclusion is unclear. These reports would demonstrate the concrete need for data centre build-out in the EU and support adjusting targets such as the tripling of data centre capacity in the EU.

03 **Public sector risk assessments (Article 29).** Member States and Union entities should publish a non-confidential summary of each assessment, covering at least the number of activities assessed per sector and the Union assurance level assigned to each category; the expected demand for services at each level; and the categories of services or components for which no suitable offer was identified.

04 **Procurement monitoring (Article 33).** Member States' annual reports should be published, and the Commission should consolidate them into a Union-wide scoreboard showing progress towards the 25% objective.

A. Reporting and monitoring obligations of Member States and the Union

# A.3 Protection of whistleblowers reporting infringements of the cloud computing sovereignty framework

The cloud computing sovereignty framework relies largely on what providers declare about themselves and their supply chain. Those best placed to know whether those declarations are true are the people working for providers, their subcontractors, their suppliers and their auditors. We therefore recommend that the co-legislators ensure that persons who report infringements of the framework are protected under Union law.

As drafted, the proposal is silent on this point. A provider may lose its recognition where it "intentionally or negligently, supplied incorrect or misleading information" (Article 17(11)), and must notify any change that may affect its recognition (Article 23(1)). Yet nothing protects the employee or contractor who reveals:

- that a statement of conformity or audit evidence is false;
- that a third country controls the provider or a subcontractor;
- that a remote feature able to disrupt the service exists;
- that a third country has obtained access to customer data.

Directive (EU) 2019/1937 on the protection of whistleblowers applies only to the Union acts listed in its Annex, and the proposal is not among them. Protection would therefore depend on indirect legal routes and on diverging national laws. Explicitly extending whistleblower protection to a new regulation is established practice in Union digital law: Article 87 of the Artificial Intelligence Act and Article 43 of the Digital Markets Act both provide that Directive (EU) 2019/1937 applies to the reporting of infringements of those regulations. The same solution would suit this proposal: it creates no new regime and relies entirely on rules Member States already apply.

**Proposed changes:**

01 **New article (Title IV), "Reporting of infringements and protection of reporting persons".** Provide that Directive (EU) 2019/1937 applies to the reporting of infringements of this Title and to the protection of persons reporting such infringements.

02 **Scope of the new article (whole of Title IV).** Ensure the article covers the whole of Title IV, and not only Chapter I as Article 24 on penalties does, so that it also applies to the assessments and the procurement obligations and derogations in Articles 29, 30, 31 and 32.

03 **Competent authorities (Article 25).** Provide that the national competent authorities designated under Article 25 are competent to receive and follow up on such reports.

04 **New recital (after recital 58).** State that persons reporting infringements of the sovereignty framework should be protected under Union law.

B. Private sector assessment of dependencies

# B.1 Mandatory assessment of dependencies by private operators of essential services

Article 31 is narrower than Article 29 – only the critical sectors listed in Annex I of the NIS2 Directive, against Annexes I and II for the public sector – and optional unless the Commission decides otherwise. We invite the co-legislators to **make the assessment mandatory** for private entities operating in the sectors of both Annexes. This would rebalance the treatment of public and private entities competing with comparable services on the same market, and it would:

- fill a gap: private operators in critical sectors relying on services that are not assessed against third-country control and data access represent a public order and national security risk just as public entities do;
- narrow the grey zone: the distinction between public and private entities is sometimes unclear (hospitals, universities, publicly owned companies with private shareholders), and an obligation on both sides of the line removes the incentive to litigate it.

Two points of design matter. The obligation is a disclosure obligation, not a purchase obligation: an operator whose assessment concludes that its arrangements are adequate has met it. And it should be integrated into the risk-management measures these entities already apply under Article 21 of the NIS2 Directive, including on supply chain security, and be proportionate to their size – a dimension added to an existing exercise, not a new one.

**Proposed changes:**

01 **Obligation and scope (Article 31(1)).** Replace "Entities referred to in Annex I of Directive (EU) 2022/2555 who are not public sector bodies may carry out similar assessments" with an obligation on entities in Annexes I and II of that Directive that are not public sector bodies to carry out such assessments, integrated into the measures they apply under Article 21 of that Directive and proportionate to their size.

02 **Reserve power (Article 31(3)).** Delete paragraph 3, which becomes redundant once the assessment is mandatory.

03 **Transmission and confidentiality (Article 31, new paragraph).** Require the results to be transmitted to the competent authority under Directive (EU) 2022/2555 and, in aggregate, to the Commission, with safeguards for commercially sensitive information.

04 **Heading and terminology (Article 31).** Align the article's "impact assessments" with the "risk assessments" of Article 29, which it cross-refers to, so that one exercise has one name.

B. Private sector assessment of dependencies

# B.2 A right for private operators to obtain supply chain information

Unlike the national authorities that conduct the risk assessments of Article 29, private operators do not always have the legal power to oblige their providers to share information on third-country control or data access, unless that right is written into the contract. Article 31(1) remains ambiguous on this point: private entities may carry out assessments without the text defining the methodology or the data to be gathered – Article 31(2) only allows the Commission to adopt a methodology at a later stage – and without any right to request information from their providers, subcontractors or component suppliers, or any obligation on those parties to provide it. The Communication accompanying the package itself promises "tools for private and public organisations to assess the sovereignty of their digital value chains"; an assessment cannot be carried out without the information it needs.

We therefore encourage the co-legislators to empower private operators with clear **rights to information** concerning third-country control, data access, supply chain measures and service continuity, and to give the assessment a defined methodology.

**Proposed changes:**

01 **Right to information (Article 31, new paragraph).** Give entities carrying out an assessment a right to obtain from their cloud computing service providers, and from those providers' subcontractors, the information needed to assess the elements listed in Article 29(2) and the criteria in Annex II – third-country control, data access, supply chain measures and service continuity – and an obligation on providers to supply it within a defined period.

02 **Methodology (Article 31(2)).** Replace the Commission's option to "issue guidance" with an obligation to adopt the methodology and templates for these assessments by implementing act, within the same deadline as the methodology under Article 29(3), drawing on the Commission's own Cloud Sovereignty Framework.

03 **Purpose and scope (Article 31(1)).** State the objective of the assessment – identifying third-country control, data access, supply chain and continuity risks – and its scope, so that the right to information is bounded and proportionate.

# Sources and resources


1. European Commission, Proposal for a Regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act), COM(2026) 502 final, 2026/0138 (COD), 3 June 2026. https://ec.europa.eu/newsroom/dae/redirection/document/129111
2. Synergy Research Group, "European Cloud Providers' Local Market Share Now Holds Steady at 15%", 24 July 2025. https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15
3. Synergy Research Group, 24 July 2025, as above.
4. European Commission, Impact Assessment Report accompanying the proposal for a Chips Act 2.0, SWD(2026) 504 final, Part 1/3, 3 June 2026, p. 42. https://ec.europa.eu/newsroom/dae/redirection/document/129106
5. European Commission, Communication on European Tech Sovereignty, accompanied by an EU Open Source Strategy, COM(2026) 503 final, 3 June 2026, p. 3. https://ec.europa.eu/newsroom/dae/redirection/document/129100
6. European Commission, Impact Assessment Report accompanying the proposal for a Cloud and AI Development Act, SWD(2026) 502 final, Part 1/2, 3 June 2026, p. 16. https://ec.europa.eu/newsroom/dae/redirection/document/129113
7. SWD(2026) 502 final, Part 1/2 (CADA impact assessment), as above, p. 11.
8. SWD(2026) 502 final, Part 1/2 (CADA impact assessment), as above, p. 25, footnote 84.
9. United States Code, Title 18, § 2713 "Required preservation and disclosure of communications and records" (added by the CLOUD Act, Pub. L. 115–141, 23 March 2018), Office of the Law Revision Counsel, US House of Representatives. https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title18-section2713&num=0&edition=prelim
10. Synergy Research Group, 24 July 2025, as above.
11. Eurostat, "53% EU enterprises used paid cloud services in 2025", news item, 3 February 2026. https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20260203-1
12. SWD(2026) 502 final, Part 1/2 (CADA impact assessment), as above, p. 11.
13. European Commission, Impact Assessment Report accompanying the proposal for a Cloud and AI Development Act, SWD(2026) 502 final, Part 2/2 (Annexes), 3 June 2026, p. 215. https://ec.europa.eu/newsroom/dae/redirection/document/129114
14. CBRE, European Data Centres Figures Q2 2026, 17 August 2026. https://www.cbre.com/insights/figures/european-data-centres-figures-q2-2026
15. Gartner, "Gartner Says Worldwide Sovereign Cloud IaaS Spending Will Total $80 Billion in 2026", press release, 9 February 2026. https://www.gartner.com/en/newsroom/press-releases/2026-02-09-gartner-says-worldwide-sovereign-cloud-iaas-spending-will-total-us-dollars-80-billion-in-2026
16. Netherlands Court of Audit (Algemene Rekenkamer), Dutch central government in the cloud: Dark clouds looming, report, 15 January 2025, p. 6. https://english.rekenkamer.nl/site/binaries/site-content/collections/documents/2025/01/15/dutch-central-government-in-the-cloud/Dutch+central+government+in+the+cloud.pdf
17. Netherlands Court of Audit, Dutch central government in the cloud, 15 January 2025, as above, p. 7.
18. Netherlands Court of Audit, Dutch central government in the cloud, 15 January 2025, as above, p. 33.
19. Netherlands Court of Audit, Dutch central government in the cloud, 15 January 2025, as above, p. 21.
20. Cour des comptes, Les enjeux de souveraineté des systèmes d'information civils de l'État, S2025-1479, 31 October 2025. https://www.ccomptes.fr/sites/default/files/2025-10/20251031-S2025-1479-Enjeux-souverainete-des-SI-civils-de-l-Etat.pdf
21. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA), Article 28(3). http://data.europa.eu/eli/reg/2022/2554/oj
22. European Supervisory Authorities (EBA, EIOPA and ESMA), "The European Supervisory Authorities designate critical ICT third-party providers under the Digital Operational Resilience Act", press release, 18 November 2025. https://www.esma.europa.eu/press-news/esma-news/european-supervisory-authorities-designate-critical-ict-third-party-providers
23. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), Article 21(2), point (d). http://data.europa.eu/eli/dir/2022/2555/oj
24. COM(2026) 503 final (Communication on European Tech Sovereignty), as above, p. 3.
25. COM(2026) 503 final (Communication on European Tech Sovereignty), as above, p. 18.
26. COM(2026) 503 final (Communication on European Tech Sovereignty), as above, p. 22, footnote 85.
27. European Commission, "Sovereign Cloud Framework explained", news item, 1 June 2026. https://commission.europa.eu/news-and-media/news/sovereign-cloud-framework-explained-2026-06-01_en
28. European Commission, "Commission advances cloud sovereignty through strategic procurement", news item, 17 April 2026. https://commission.europa.eu/news-and-media/news/commission-advances-cloud-sovereignty-through-strategic-procurement-2026-04-17_en
29. European Commission, "Sovereign Cloud Framework explained", 1 June 2026, as above.
30. SWD(2026) 502 final, Part 1/2 (CADA impact assessment), as above, p. 25.
31. SWD(2026) 502 final, Part 2/2 (CADA impact assessment, annexes), as above, pp. 97 and 121.
32. Regulation (EU) 2022/2554 (DORA), as above, Article 28(3).
33. Regulation (EU) 2024/1252 of the European Parliament and of the Council of 11 April 2024 establishing a framework for ensuring a secure and sustainable supply of critical raw materials (Critical Raw Materials Act), Article 20(3) and (4). http://data.europa.eu/eli/reg/2024/1252/oj
34. SWD(2026) 502 final, Part 2/2 (CADA impact assessment, annexes), as above, pp. 214 and 216.
35. European Commission, Executive Summary of the Impact Assessment Report accompanying the proposal for a Cloud and AI Development Act, SWD(2026) 503 final, 3 June 2026, p. 2. https://ec.europa.eu/newsroom/dae/redirection/document/129115
36. SWD(2026) 502 final, Part 2/2 (CADA impact assessment, annexes), as above, Table 41, p. 129.
37. SWD(2026) 502 final, Part 2/2 (CADA impact assessment, annexes), as above, p. 15.
38. Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, Article 2(1)(a) and Annex. http://data.europa.eu/eli/dir/2019/1937/oj
39. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), Article 87. http://data.europa.eu/eli/reg/2024/1689/oj
40. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act), Article 43. http://data.europa.eu/eli/reg/2022/1925/oj
41. Directive (EU) 2022/2555 (NIS2), as above, Article 21(2), point (d).
42. COM(2026) 503 final (Communication on


FOTI