

OCTOBER 2026



BSA Position Paper on the Cloud and AI Development Act

**Enabling a competitive, open, and resilient
European cloud and AI ecosystem**

The Business Software Alliance (BSA) is the leading advocate for the global software industry before governments and in the international marketplace. Our members¹ are at the forefront of software-enabled innovation that is fueling global economic growth, including cloud computing and AI products and services.

BSA's membership includes many of the world's leading enterprise software providers to organizations of all sizes. Enterprise software companies provide the trusted foundation for responsible use of artificial intelligence (AI). Throughout the years, our members have heavily invested in creating cutting-edge solutions that support digital transformation across all industries and sectors in Europe.

BSA and its members welcome the European Commission's ambition to strengthen Europe's cloud and AI ecosystem, investment, and infrastructure through the Cloud and AI Development Act (CADA). We support the EU's goal to build economic resilience, foster homegrown European technology companies and scale a competitive domestic digital industrial base. We also believe that the proposal's focus on research, development and innovation, and autonomy can help Europe expand sustainable data center capacity, accelerate cloud and AI adoption in strategic sectors, and support the objectives of the AI Continent Action Plan.

However, in our view, to achieve these objectives **CADA should follow a genuinely risk-based approach** that truly fosters resilience and cybersecurity, rather than reducing the choices of EU users. We think that this can be done best by preserving the openness of the European cloud market while strengthening its sovereignty and competitiveness, in line with the Commission's objectives.

In particular, our concern is that several provisions of CADA as proposed would undermine the Commission's goals by restricting the pool of digital services providers available to public sector entities, increasing compliance costs without a corresponding security benefit, and introducing nontechnical origin-based criteria that would reduce competition without reliably improving resilience. Instead, if the EU really wants to strengthen its cloud and AI ecosystem, it needs to adopt a different, more pragmatic approach that increases capacity, removes barriers to deployment, and keeps Europe open to trusted partners.

Furthermore, Europe is not only a consumer of software and cloud services; it is also a global provider, whose companies—many of which are BSA members—export state-of-the-art technologies worldwide. CADA should support competitiveness, simplification, and innovation, rather than introduce defensive rules that artificially reduce competition within the Internal Market or add layers of red tape for contracting authorities and applicants to tenders.

In the specific framework of CADA, BSA supports measures that promote investment, interoperability, cybersecurity, secure data flows, digital skills, and innovation. Genuine digital sovereignty should be built on strong standards, transparent governance, demonstrable security,

¹ BSA's members include: Adobe, Alteryx, Amadeus, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., TrendAI, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

and the ability to manage risk in an open and interconnected digital ecosystem. At BSA, we believe that Europe should strengthen its autonomy by further building its digital capabilities up, and not by shutting partners out. CADA should avoid creating discriminatory market access conditions, duplicative compliance obligations, or procurement rules that limit choice for public sector entities and businesses.

A preliminary concern cuts across the entire framework. The revision process of the Public Procurement Directives has followed the release of the Cloud and AI Development Act proposal. As a result, CADA risks introducing a *lex specialis* procurement regime (with its own eligibility criteria, assurance levels, award criteria, and governance architecture) before the *lex generalis* has been updated. Legislating a detailed sovereign cloud procurement framework in advance of the revision of broader public procurement rules creates a structural sequencing problem: **CADA will embed specific procurement rules that may be inconsistent with the general procurement reform.** Contracting authorities across 27 Member States will be required to apply CADA's sovereignty procurement rules to cloud contracts while simultaneously awaiting revised general procurement rules that may set different requirements for the same contracts. This risks creating transitional confusion, legal uncertainty, and compliance costs that fall on both buyers and providers without corresponding policy benefit. Co-legislators should ensure that CADA's procurement provisions are explicitly designed to be consistent with and complementary to the Public Procurement Regulation, and that the two instruments are sequenced or reconciled in a way that gives contracting authorities a coherent, workable legal framework from the outset.

BSA RECOMMENDS:

- 1 Addressing CADA's Broader Structural Issues page 4
- 2 Preventing Assurance Levels From Becoming Market Access Barriers..... page 7
- 3 Avoiding Fragmentation Through Clear Rules and Consistent EU Governance..... page 12
- 4 Implementing Workable Non-Price Criteria to Determine Union Added Value page 15
- 5 Building Real Security, Not Redundant Audits page 16
- 6 Maintaining Defined Boundaries Between CADA and NIS2..... page 18
- 7 Using Trusted Partnerships as a Tool to Strengthen Resilience..... page 19

Address CADA's Broader Structural Issues

Keeping the CADA Framework Risk-Based and Predictable

The European Commission presented CADA as a framework to expand Europe's cloud and AI capacity, simplify deployment, and maintain an open market for trusted partners. These objectives, however, are undermined by the design of the proposed assurance framework under Title IV and Annexes II and III.

Broadly speaking, **the framework conflates security with corporate origin**, creating a risk that legitimate resilience objectives restrict the options available to EU users and lead de facto to market access restrictions based on nationality, ownership, or supply-chain origin. This reflects a fundamental design flaw: **a provider's ability to protect EU government data from unauthorized foreign government access depends on its technical, legal, and organizational safeguards, and not on where its ultimate parent company is incorporated.** To preserve innovation, choice, and proportionality, CADA should therefore clearly limit the scope of Title IV by relying on existing risk-based cybersecurity frameworks, rather than imposing prescriptive sovereignty requirements.

If anything, **an appropriate resilience strategy would consist of obliging users to enhance supply-side diversity rather than replacing non-EU providers with EU-only providers.** A non-EU-headquartered provider operating EU data centers, using EU law-governed contracts, employing EU-resident personnel, and implementing robust technical controls against foreign government access may present a more secure option than a provider with weak protections and no operational separation. Moreover, the recent wars in Ukraine and the Middle East have demonstrated that the ability to transfer data across geographically distributed data centers can be essential to protect it against physical and cybersecurity attacks, and to offer more security than on-prem or geographically limited solutions.

Furthermore, **the assurance framework created under Article 16 and Annexes II and III should be stable, predictable, and set by the co-legislators to preserve legal certainty.** Under the current proposal, the Commission could tighten criteria post-adoption without returning to Parliament or Council for fresh legislative authority, subject only to a passive non-objection mechanism with a two-month window. However, should Annexes II and III be subject to amendment every 18 months via delegated acts, the lack of certainty would affect all types of companies, regardless of their origin, size, or business model.

The fact that an organization may unexpectedly be subject to new or additional data sovereignty requirements could produce a distortive effect on their selection of cloud providers, leading industries that are only potentially in scope to act as if they were de facto subject to the same

A provider's ability to protect EU government data from unauthorized foreign government access depends on its technical, legal, and organizational safeguards, and not on where its ultimate parent company is incorporated.

requirements, given the time and resources required to migrate to a new system, even under the cloud-switching terms of the EU Data Act. In practice, this means that **a provider certified at Level 2 today could find itself ineligible for the same contracts in three years if the delegated acts tighten the criteria beyond what it can meet.**

Infrastructure investment, cloud architecture decisions, and public procurement planning operate on cycles of five to 10 years. **A compliance framework that can be materially altered every 18 months without legislative oversight is structurally incompatible with those investment timelines. Businesses cannot invest at scale if the legal conditions for market access can shift before a data center project, migration program, or certification process is completed.** And business uncertainty would lead to less investment in digital innovation, which in turn would make meeting the EU's Digital Decade targets more challenging.

BSA therefore recommends that the primary text establish that Annex II and III criteria remain risk- and behavior-based as a binding constraint on future amendments, that they remain subject to the ordinary legislative procedure, and that any amendment to the criteria be subject to a mandatory impact assessment and a minimum 24-month transition period before taking effect.

Setting Reasonable Expectations on Cross-Border Lawful Access Practices

Some of the premises of CADA seem to be built on the assumptions that EU companies will never be subject to foreign requests for governmental access to data, and that cross-border governmental access to data should be impermissible. Both assumptions are flawed.

Indeed, governments across the world can request or oblige private actors, notably in the digital sphere, to grant access to data for law enforcement or national security purposes. Provided that this happens under appropriate safeguards, such access can be perfectly legitimate and does not amount to "surveillance." International guidance, such as that delivered by the Organisation for Economic Co-operation and Development, sets out relevant safeguards and boundaries for lawful access to data. Given the international scope of many digital actors, such access can also happen in a cross-border modus. Just as the US Cloud Act is by no means exceptional in that regard, the EU eEvidence Regulation also allows European authorities to require digital providers to deliver cross-border data access for law enforcement purposes. In particular, Article 1 of the eEvidence Regulation states that its rules apply "regardless of the location of the data," effectively allowing cross-border enforcement of the law.

Assuming that EU-originating companies will never be subject to non-EU laws would be equally unrealistic. For instance, a [Legal Memo from Greenberg-Traurig to the Dutch Government](#) sets out very clearly that depending on the degree of minimal contacts, European companies are also exposed to the reach of the US Cloud Act. Similarly, [OVH's own website](#) states that "[A]s a global, hyper-scale cloud provider" it will comply with US law and "[u]nder the CLOUD Act, that could include data stored outside of the United States." In a recent Canadian case, the Canadian Ontario Court of Justice compelled OVH France to disclose data stored in France. **The more successful EU digital companies become, the more they expand globally, the higher their exposure under foreign laws will become.**

Avoiding Barriers That Undermine the Competitiveness of EU-Based Companies

Beyond legal certainty, the design of the assurance levels as it stands risks penalizing the very companies Europe may want to grow: innovative providers with global operations, international customers, cross-border supply chains, and the ability to scale. **A European cloud or software company that expands globally should not become less eligible to serve European public sector customers because it has succeeded outside of Europe**, and yet, this is a concrete risk presented by the CADA proposal at this stage. Additionally, assurance levels 2 and above would only be accessible by paying for auditing costs that would effectively cut a large share of companies out of the market.

To make matters worse, **European cloud providers would have difficulties qualifying for any assurance level, regardless of their size**, because most cloud providers, including European ones, rely on international supply chains for both software and hardware. Modern software is built on a complex ecosystem of third-party technologies. Preventing companies from integrating such technologies into their stacks solely because they may involve cross-border data transfers would weaken product development. The same consideration applies to open-source software. Moreover, given the references to metadata and subcontractors in Annex II, the impact of assurance levels could extend well beyond the public procurement of cloud services, affecting the broader cloud value chain.

If applied broadly, these requirements risk cutting Europe out of the global cloud market, rather than keeping global cloud providers out of Europe. All in all, **this would result in most European cloud or software companies being unable to provide services to European public sector entities**—exactly the opposite of what CADA is seeking to achieve.

Different Services, Same Rules?

A further structural problem is that CADA's compliance architecture does not adequately account for the diversity of cloud service delivery models: indeed, the framework seems to be built around the concept of Infrastructure-as-a-Service (IaaS), but that is not the only type of cloud or AI services that European public sector entities procure. On the contrary, European public sector entities rely on a wide range of cloud-based services day-to-day, for instance enterprise applications, productivity tools, HR and financial management systems, document processing tools, back-up, and sector-specific platforms. Each of those carries distinct technical architectures, operational models, and risk profiles. A uniform framework applied without differentiation to these highly different delivery models and applications risks producing unworkable compliance requirements for the services that public sector entities depend on most.

The challenge is particularly acute for services delivered through continuously evolving software stacks that are updated, patched, monitored, and supported by distributed engineering organizations. The distinction between development and operational support, which is central to the personnel localization criteria, is not a clearly defined operational boundary for many cloud service providers. Every software update, every security patch, every change to application logic deployed to a production environment potentially engages the personnel localization criteria in ways that the current text does not resolve. A bug fixed by an engineer outside the EU, deployed to a certified environment, touches that boundary in a way that has no clear answer under the draft CADA proposal.

BSA therefore urges co-legislators to **request the Commission to publish specific guidance on how the assurance level criteria apply across different cloud service delivery models and applications before CADA enters into application.** The Commission should also consider whether differentiated compliance pathways with, for instance, obligations calibrated to the actual risk profile and delivery architecture of the service are appropriate. The goal should be **a framework that is genuinely workable across the full range of cloud services that public sector entities procure, not one that creates legal uncertainty** at precisely the point where public sector digital transformation depends most on clarity.

BSA RECOMMENDS:

- » **Establishing in the Regulation that Annex II and III criteria must remain risk and behavior-based** as a binding constraint on future amendments, that they must remain subject to the ordinary legislative procedure, and that **any amendment to the criteria must be subject to a mandatory impact assessment and a minimum 24-month transition period before taking effect;**
- » Requesting that the Commission release **specific guidance on how assurance-level criteria apply across different cloud service delivery models and applications.** Such guidance should be made available before CADA enters into application; and
- » **Limiting the overall scope of Title IV** by relying on existing risk-based cybersecurity frameworks, instead of creating new prescriptive sovereignty requirements.

2

Prevent Assurance Levels From Becoming Market Access Barriers

Avoiding Disproportionate Data Localization Requirements

CADA should adopt **proportionate, risk-based criteria**; accordingly, assurance level 1 should avoid requirements, such as data localization, that are disproportionate to the risks they are supposed to address. Comparable assurance frameworks are materially narrower in scope: France's SecNumCloud framework does not apply indiscriminately to all public sector cloud use, while FedRAMP is limited to federal agency procurement use cases and contains express out-of-scope categories, reflecting a less expansive and less prescriptive model than CADA's proposed baseline.

Data localization requirements are liable to reduce the resilience of digital infrastructure during large-scale disruptions, namely by limiting the ability of organizations to distribute or replicate data across jurisdictions. As an example, during the widespread power outage that affected Spain

and Portugal in April 2025, organizations relying on infrastructure confined to Spain had fewer options for disaster recovery than those using geographically distributed, multi-country cloud architectures.

Similarly, on 1 March 2026, amid the escalating conflict between Iran and Israel, objects, widely attributed to missile and drone strikes on the United Arab Emirates, struck an AWS data center in the country, causing sparks and a fire that led local authorities to cut power and take an entire Availability Zone offline. Organizations subject to UAE data localization requirements, unable to fail over to infrastructure outside the country, faced significant disruptions to banking, payments, and other services.

These outages illustrated how **restrictions on cross-border data storage or replication can reduce operational flexibility and make it more difficult to maintain service continuity during regional infrastructure failures.**

Moreover, **data localization requirements may weaken, rather than strengthen, data security and data privacy.** By constraining an organization's ability to distribute and replicate information across multiple jurisdictions, localization requirements concentrate data within a single location, creating a more valuable and more attractive target for malicious actors than a geographically distributed architecture would present.

The requirement to localize telemetry and metadata within the Union, which are present even at Level 1, the universal floor for all public sector cloud procurement, creates a further and more acute problem: it **directly degrades the cybersecurity posture of the services it is supposed to protect.** This is not a compliance cost issue. It is a security issue that goes to the heart of CADA's stated resilience objectives.

Modern cybersecurity operations depend structurally on cross-border data flows. Security Operations Centers operate on a follow-the-sun model, rotating analyst coverage across time zones to ensure that awake, available, and appropriately skilled teams can respond to incidents in real time, 24 hours a day. This is compounded by the requirement to fully localize tech and operational support at Level 2, without any possibility for escalations. Requiring that telemetry and metadata remain within the Union means that analysts and systems analyzing traffic located outside the EU cannot access the signals they need to detect, investigate, and respond to incidents affecting EU-based infrastructure. The practical effect is a degradation in incident response capability: incidents taking longer to be detected, slower containment, and greater damage from attacks that could have been stopped earlier.

The problem goes deeper than staffing. **Effective threat detection relies on the correlation of signals across global datasets.** An attack pattern first detected in one region (e.g., a new ransomware variant, a novel phishing campaign, a previously unknown vulnerability being actively exploited) is identified and characterized by correlating telemetry from across the provider's global infrastructure. That characterization then updates protection rules for all customers globally within minutes. **If EU-based telemetry could not flow to global security intelligence systems, EU public sector customers would effectively be cut off from this real-time global threat intelligence.** They would receive protection that is calibrated to threats observed within the EU only, which would represent a significantly degraded security posture compared to what a globally integrated security architecture provides.

Localization requirements concentrate data within a single location, creating a more valuable and more attractive target for malicious actors than a geographically distributed architecture would present.

The same applies to forensic incident response. When a major incident occurs within EU infrastructure, the most capable specialist teams (malware analysts, forensics experts, reverse engineering specialists) may be located outside the EU. Indeed, an organization's own personnel may themselves be temporarily located outside the EU, whether traveling for business or working remotely, at the moment an incident occurs. Preventing those teams from accessing relevant telemetry data in the course of an incident response would not protect the data. It would simply slow the response and increase the damage. **This would be the opposite of the resilience outcome CADA claims to pursue.**

BSA therefore recommends that the telemetry and metadata localization requirements be removed from Level 1 altogether. Localization requirements should not be used as a proxy for security. Alternatively, localization requirements could be replaced with a governance-based obligation: **providers could be asked to demonstrate that access to telemetry and metadata meets the requirements of due process under EU law, that any access from outside the EU is logged, auditable, and subject to contractual restriction, and that measures are in place to prevent third-country government access without legal authorization.** This approach would achieve a legitimate sovereignty objective without degrading the cross-border security intelligence capabilities that effective cybersecurity requires.

Encryption as a Sovereignty Guarantee

CADA's assurance framework should explicitly recognize technical safeguards as meaningful sovereignty guarantees in their own right and not treat corporate control as the only relevant criterion. Customer-managed encryption architectures, including Bring Your Own Key (BYOK) and Keep Your Own Key (KYOK) models, provide a concrete, auditable, and verifiable guarantee against unauthorized data access that operates independently of the provider's corporate structure. Under a BYOK or KYOK model, the provider physically cannot access readable customer data and cannot produce readable data in response to a foreign government compulsion order, because the decryption keys are held exclusively by the customer or by a customer-designated third party within the EU. **This is precisely the outcome CADA claims to pursue but achieved through technical architecture rather than corporate ownership tests.**

The failure to recognize encryption-based protections as a relevant mitigating factor at Levels 3 and 4 is a significant design flaw in the current proposal. A non-EU-headquartered provider that operates KYOK architecture for a public sector customer, where the keys are held by an EU-established key management service under EU-law-governed arrangements, provides stronger practical data protection against foreign government compulsion than a nominally EU-controlled provider that does not implement equivalent technical safeguards. CADA's framework as designed would exclude the former and include the latter, producing a worse security outcome in the name of sovereignty.

A non-EU-headquartered provider that operates KYOK architecture for a public sector customer, where the keys are held by an EU-established key management service under EU-law-governed arrangements, provides stronger practical data protection against foreign government compulsion than a nominally EU-controlled provider that does not implement equivalent technical safeguards.

BSA therefore recommends that Annex II criteria at all assurance levels explicitly recognize customer-managed encryption key architectures (including BYOK and KYOK models) as a relevant and meaningful technical safeguard against unauthorized data access, and that providers implementing such architectures receive appropriate credit in the assurance level assessment process. **The criteria should be amended to evaluate encryption architecture, key custody arrangements, and demonstrated technical inability to produce readable data in response to third-country government requests as primary indicators of data sovereignty, rather than or alongside corporate control tests.**

Creating a Narrow, Coherent Definition for the Notion of “Subcontractors”

The term “subcontractor” in CADA’s Annex II creates legal ambiguity. As currently drafted, sovereignty criteria apply uniformly to all entities involved in the provision of the audited service *“without differentiation based on role, data access, or actual impact on service security and continuity.”* This creates disproportionate compliance burdens and audit requirements that are neither proportionate to the risks involved nor matched by meaningful gains in security assurance.

BSA recommends co-legislators to adopt a clear, narrow definition of “subcontractor” limited to entities that have access to, or could affect the confidentiality or integrity of, customer data or classified information processed under the audited service—directly reflecting CADA’s sovereignty rationale and ensuring that localization and audit obligations fall where the actual risk lies, rather than across the broader technology supply chain on which any modern cloud service necessarily depends. Such definition should be aligned with other relevant EU legislation, such as the Digital Operational Resilience Act (DORA).

Level 4: A Separate and More Acute Problem

Level 4 raises a distinct and more acute concern. Unlike Level 3, it contains no recognition pathway for non-EU-controlled providers whatsoever, not even a discretionary one. The effective control criterion in Annex II Level 4(i)(ii) additionally requires that no third-country entity exercise effective control over the design, development, maintenance or evolution of software components used in the service. As drafted, this criterion is incompatible with how modern software ecosystems operate. In addition, critical open-source tooling (including widely used infrastructure components governed by global foundations with significant non-EU participation) would be excluded under this standard.

Level 4 would also have a de facto impact on hardware supply chains. Although the relevant criteria are framed around “software,” the definition appears to incorporate the approach adopted under the Cyber Resilience Act, in which the notion of “software” includes the firmware

necessary for hardware to function. This reflects a misunderstanding of how software is built and governed. Indeed, the European Commission has confirmed that Level 4 supply-chain controls would not stop at application or infrastructure software but would extend to the hardware providers whose firmware is embedded in the relevant cloud stack. In practice, this would make Level 4 requirements even more difficult to fulfill: a provider would need not only EU-controlled software development and maintenance, but also hardware and firmware supply chains capable of satisfying the same origin-based constraints. Such conditions would of course make Level 4 either completely unattainable for any software provider (European and non-European) operating a modern technology stack, or available only at significant cost and with limited choice.

Level 4 criteria should therefore be redrafted to address the actual security risk, rather than governance participation structures that do not determine security outcomes.

BSA RECOMMENDS:

- » **Recognizing customer-managed encryption key architectures** (including BYOK and KYOK models) **as relevant and meaningful technical safeguards against unauthorized data access for all assurance levels under Annex II.** Specifically, encryption architecture, key custody arrangements, and demonstrated technical inability to produce readable data in response to third-country government requests should be assessed as primary indicators of data sovereignty, rather than corporate control tests;
- » **Clarifying the notion of “subcontractors” under Annex II**, limiting it to entities that have access to, or could affect the confidentiality or integrity of, customer data or classified information processed under the audited service. Such definition should be aligned with other relevant EU legislation;
- » **Ensuring that Assurance Level 1 criteria remain proportionate to the level of risk**, therefore removing criteria such as telemetry and metadata localization requirements. Alternatively, localization requirements may be replaced with governance-based obligations, such as allowing providers to demonstrate that access to telemetry and metadata meet the requirements of due process under EU law;
- » **Rewriting the Levels 3 and 4 criteria in Annex II to be exclusively risk- and behavior-based** (i.e., evaluating what technical, legal and organizational controls a provider operates to prevent unauthorized data access and service disruption, rather than where its parent company is incorporated). The current origin-based exclusions at Levels 3 and 4 must be removed and replaced with auditable behavior-based requirements that any provider can meet regardless of corporate origin, provided it demonstrates the required security posture; and
- » **Introducing a recognition pathway at Level 4 for non-EU-controlled providers** that can demonstrate through technical audit that no third-country entity can access data or compel service disruption, consistent with the behavior-based logic that should govern all four assurance levels.

Avoid Fragmentation Through Clear Rules and Consistent EU Governance

Clarifying the Scope of CADA Through Appropriate Definitions

Title IV of CADA relies on several concepts that are central to market access but insufficiently defined. Terms such as “public order,” “critical use cases,” and the criteria for assigning assurance levels must be clear and non-discriminatory. **Vague political objectives cannot substitute legal definitions** when public procurement, service eligibility, and long-term investment decisions are at stake.

The same logic should apply to the broader interaction between CADA and other recent or forthcoming EU initiatives, including EUCS, the future Public Procurement Act, and the AI Act: **the Commission should clarify how CADA fits within the wider legislative framework for cloud and AI**, and ensure that key definitions, such as “AI agents,” remain aligned with relevant horizontal legislation.

Building a Consistent Governance Framework

The division of responsibilities between Member States, national authorities, auditors, and the Commission also needs to be clarified. In the current proposal, Member States would determine which assurance levels would apply to which public sector activities, national authorities would recognize assurance levels, auditors would assess providers, and the Commission may later specify methodology or even required assurance levels through implementing acts. This creates too many disparate decision points and too much room for divergence.

If the EU creates a sovereignty framework, it should be genuinely European. This requires clear and consistently applied criteria for assigning assurance levels, alongside EU-wide recognition of the assurance status achieved by providers. While Member States may reach different risk-based determinations regarding the assurance level appropriate to particular public sector activities, providers should not face duplicative or inconsistent national processes for demonstrating that they meet a given assurance level. Greater consistency in the framework would benefit both Member States and companies:

- » For Member States, by providing a common framework and greater certainty when sharing data and services across borders.
- » For service providers, by ensuring that an assurance level achieved in one Member State is recognized across the European Union.

A company providing a service in one Member State should be able to provide the same service in another Member State via mutual recognition of businesses’ respective assurance levels, thereby fully exercising the freedom to provide services protected under EU treaties. And the rules for

While Member States may reach different risk-based determinations regarding the assurance level appropriate to particular public sector activities, providers should not face duplicative or inconsistent national processes for demonstrating that they meet a given assurance level.

revocation, appeal, remediation, and contract continuity should be at the very least harmonized from the start, unlike what Article 24 foresees by requiring Member States to individually lay down rules to respond to infringements related to breaches of auditing requirements.

The Commission's override power under **Article 29(5) addresses inadequate assessments but risks creating an upward ratchet in assurance levels without sufficient safeguards to ensure that requirements remain proportionate and risk based.** The risk assessment methodology, which will determine in practice what proportion of public sector workloads are pushed to Levels 3 and 4, has not yet been written and is currently expected to be set by implementing acts after adoption. Until that methodology exists and is subject to adequate stakeholder consultation, the practical scope of the assurance framework, and therefore the effective scope of the market access restrictions, remains genuinely unknown.

Embedding Criteria for Market Access Into the Regulation to Ensure Legal Certainty

The concern about legal certainty goes beyond the 18-month review cycle highlighted in section 1 of the present paper. The implementing act mechanism under Article 29(3) and (5) means that whatever is negotiated and agreed during the legislative process regarding the methodology that Member States may use to determine the appropriate risk assurance level for any given service may not remain the operative standard for long.

For this reason, Articles 29 and 30 should be revised to ground assurance levels into clear, ex ante criteria set out in the Regulation or its annexes and subject to ordinary legislative procedure. Implementing acts may support consistent application of the Regulation, but they should not be used to redefine the conditions for Member States to determine the appropriate risk assurance level for any given tender so often that it becomes impossible for companies to consistently plan their participation in public procurement for cloud services.

Moreover, achieving true sovereignty includes embracing competition and diversification as tools to strengthen resilience and economic security, in line with the EU's Competitiveness Compass. Accordingly, national interest or the simple willingness to adopt best-in-class solutions should be sufficient reason for a Member State to select the provider it considers best placed to meet its needs. To that end, **EU Member States should be able to rely on exemptions under Article 30(4) whenever they deem it necessary**, on the basis of a presumption that such decisions pursue legitimate national security and resilience objectives, without being subject to onerous evidentiary requirements.

BSA RECOMMENDS:

- » Demanding that the Commission **clarify how CADA fits within the wider legislative framework for cloud and AI**, and ensure that key definitions, such as “AI agents,” remain aligned with relevant horizontal legislation;
- » **Defining key notions** such as “public order” and “critical use cases” directly in the Regulation;
- » **Harmonizing recognition, withdrawal, appeal, remediation, and contract-continuity procedures at EU level**, including under Article 24, to avoid divergent national penalties and inconsistent enforcement across Member States;
- » **Clarifying the respective roles of Member States, national competent authorities, auditors, and the European Commission**, so that providers and public authorities know who decides, who verifies, who enforces, and who can revoke an assurance level;
- » **Revising Articles 29 and 30 so that the criteria employed by Member States to determine risk assurance levels remain grounded on clear, ex ante, risk-based rules**, with implementing acts limited to supporting consistent application rather than disrupting legal certainty;
- » **Strengthening the existing Union assurance framework through an “Assurance Level Passport” approach**, ensuring that a provider recognized as meeting a particular Union assurance level in a given Member State can rely on that status consistently across the Union, without duplicative national assessment or recognition requirements;
- » **Keeping any future changes to assurance levels subject to appropriate legislative scrutiny, stable transition periods, and clear grandfathering rules**, so that providers can plan investments and public authorities can preserve service continuity; and
- » **Clarifying that Article 30(4) derogations are available to Member States without onerous evidentiary requirements**, thus ensuring that public authorities retain access to best-in-class solutions where the certified market cannot yet meet their operational needs.

4

Implement Workable Non-Price Criteria to Determine Union Added Value

Article 32 raises significant concerns regarding the proposed mandatory use of “Union added value” as a non-price award criterion in public procurement.

Making Article 32 Optional

As a general consideration, **Article 32 should be made genuinely optional**: contracting authorities should be permitted, rather than required, to consider ecosystem contribution criteria where these are objective, transparent, proportionate, and directly linked to the subject matter of the contract. This approach would preserve flexibility for public buyers while avoiding procurement rules that fragment the market or favor particular supply chains without a demonstrable security rationale.

The only structural safeguard against Article 32 being used as a de facto European preference mechanism is the requirement in Article 32(2)(d) that Union added value criteria remain “ancillary and not decisive.” **This constraint is qualitative and entirely unenforceable in practice.** It sets no numerical threshold, provides no objective standard against which a contracting authority’s weighting decisions can be assessed, and creates no mechanism for challenge or review if a contracting authority weights the Union added value criteria at a level that effectively determines the outcome of a tender. A criterion that, according to Recital 67, carries 15 out of 120 points can in practice be decisive if the remaining criteria produce a sufficiently close result among the leading tenderers; and under current public procurement case law, a contracting authority retains significant discretion in how it applies award criteria as long as the process is transparent.

This is not a theoretical concern. It is the standard **market distortion mechanism that origin-preference criteria create in public procurement practice**: the formal weighing appears modest, but the practical effect on tender outcomes can be substantially larger than the nominal weight suggests.

BSA therefore recommends that co-legislators introduce **a binding maximum combined weighting cap for all Union added value criteria in the operative text of Article 32**—not in the recitals—and **establish a clear review mechanism**, allowing tenderers to challenge award decisions where Union added value criteria have been applied in a manner that was not genuinely ancillary to the overall assessment. Without these procedural safeguards, Article 32 will function as an origin preference in practice regardless of how it is framed in the text.

Revising Union Added Value Criteria to Reflect Genuine Security Objectives

The specific criteria that Article 32 introduces to determine Union Added Value raise further concern. While contracting authorities should be free to recognize meaningful contributions to the European ecosystem, these criteria should not become an aprioristic preference for EU-designed or EU-manufactured technology. Security, resilience, interoperability, sustainability, and value for money are legitimate procurement considerations. By contrast, **the location where a chip, server, or networking component was designed or manufactured is not, in itself, a reliable proxy for security.**

This concern is particularly acute with respect to Article 32(3)(d), which would require contracting authorities to assess the extent to which a service is delivered through critical computing, storage, and networking hardware components designed or manufactured in the Union. Given the complexity, global distribution, and interdependence of modern technology supply chains, such a requirement would be extremely difficult, if not impossible, to implement in practice and risks discriminating against secure, high-quality solutions without a corresponding security benefit.

Beyond the practical implementation difficulty of Article 32(3)(d), BSA's concern lies with the absence of any security rationale. A chip or server designed outside the Union is not less secure than one designed within it. Article 32(3)(d) is an industrial preference criterion embedded in a security instrument. BSA therefore recommends that **Article 32(3)(d) be deleted entirely**.

BSA RECOMMENDS:

- » **Making Article 32 optional for contracting authorities**, who should be permitted but not required to apply ecosystem contribution criteria where these are objective, transparent, proportionate, and directly linked to the subject matter of the contract;
- » **Introducing a binding maximum cap for all Union added-value criteria in the operative text of Article 32**, allowing tenderers to challenge award decisions where Union added value criteria were granted excessive weight compared to the overall assessment; and
- » **Deleting Article 32(3)(d) in its entirety.**

5

Build Real Security, Not Redundant Audits

Grounding CADA Audits in Existing Cybersecurity Frameworks

CADA should move the needle from a narrow idea of sovereignty to a practical model of resilience. This means **focusing on whether providers can prevent, withstand, respond to, and recover from risks**. It does not mean layering new audit requirements on top of existing cybersecurity obligations without showing what additional protection they deliver.

Articles 17 and 20 to 24 would require providers seeking assurance levels 2 to 4 to undergo independent audits. BSA recognizes the value of assurance mechanisms where they are targeted and proportionate, such as under the NIS2 Directive. But in other contexts, mandatory audits for broad categories of services risk becoming a costly and time-consuming gatekeeping exercise,

especially for the smaller European providers and scale-ups that CADA should be designed to support. **A blanket audit requirement would risk becoming a compliance exercise with limited demonstrable benefits for the quality or security of the sector.**

More Competition, Fewer Audit Requirements

The EU already has a horizontal cybersecurity baseline, NIS2. NIS2 applies to cloud computing providers, data center providers, content delivery networks, managed service providers, and other digital infrastructure entities, and requires cybersecurity risk-management measures and incident reporting across critical sectors. If a provider can demonstrate compliance with NIS2, relevant EU cybersecurity schemes, and other sectoral rules, such as General Data Protection Regulation requirements, that evidence should count meaningfully toward any CADA assurance assessment, rather than be duplicated through a separate and costly CADA process. Otherwise, CADA will reward audit capacity rather than security performance, which should be a founding element of resilience-based sovereignty.

Additional audits would also fall most heavily on smaller and emerging providers, as they are not in the same position as larger companies when it comes to absorbing recurring certification costs. If CADA is intended to strengthen Europe's cloud and AI ecosystem, creating barriers that entrench incumbents or narrow down the field of competitors is unlikely to be the best way to achieve that goal.

Making Rules on Revoking Assurance Levels Consistent

CADA provisions on the consequences of revoking an assurance level also lack clarity and consistency. By leaving Member States to define the rules applicable to infringements of auditing requirements under Article 24, **CADA gives way to fragmented enforcement, divergent penalties, and reduced legal certainty across the Union.**

Providers, customers, and public authorities must know whether revocations would apply EU-wide, whether they would be temporary or permanent, which transition period would apply, and how ongoing public contracts would be protected to avoid service disruption. Without clear rules, the system will create uncertainty for the very public services it is meant to secure.

BSA RECOMMENDS:

- » **Replacing blanket audit requirements with a proportionate assurance model that recognizes existing compliance, avoids duplicative checks, and keeps SMEs and innovative providers in the market; and**
- » **Clarifying the concrete consequences, at EU level, of the withdrawal of an assurance level.**

6

Maintain Defined Boundaries Between CADA and NIS2

Preserving the Distinction Between Public Procurement and Private Markets

Article 31 grants the Commission broad powers to require private-sector entities subject to NIS2 to conduct sovereignty assessments and implement mitigation measures. If interpreted broadly, it could effectively **extend sovereign procurement requirements into ordinary commercial B2B contracts, undermining contractual freedom and open-market competition.**

NIS2 establishes the EU baseline for cybersecurity risk management and incident reporting across critical sectors, including cloud and digital infrastructure. **If CADA criteria are layered onto NIS2 entities without evidence of necessity, companies will face overlapping regimes, inconsistent supervisory expectations, and higher compliance costs without a clear security benefit.**

Keeping CADA Targeted and Proportionate

Article 31 would allow the use of CADA criteria for NIS2 entities outside the public sector. This provision goes **beyond the boundaries of the scope of the CADA proposal**: CADA is intended to address cloud and AI capacity, public sector adoption, and a public procurement-driven sovereignty framework. It should not become a backdoor mechanism for adding sovereignty obligations across the private sector.

The direction of travel should be the opposite: **NIS2, in accordance with cybersecurity certifications under the Cyber Security Act 2 (CSA2), should serve as the baseline for cybersecurity and resilience in cloud procurement, while CADA should add only targeted, proportionate requirements for clearly defined sensitive public sector use cases.** Conversely, extending CADA to private NIS2 entities would weaken the simplification agenda that Europe needs to accelerate AI and cloud uptake. Likewise, any supply chain requirements should be consistent with the ICT supply chain framework that has been proposed under CSA2 and similarly covers nontechnical risks beyond cybersecurity.

BSA RECOMMENDS:

- » **Deleting Article 31** so that the scope of CADA criteria would not be applied to NIS2 entities;
- » **Adopting NIS2 criteria as the baseline for cybersecurity and resilience in cloud procurement**, limiting CADA to targeted, proportionate requirements for clearly defined sensitive public sector use cases; and
- » **Ensuring consistency with the proposed ICT supply chain framework under CSA2** and avoiding any duplication of requirements.

7

Use Trusted Partnerships as a Tool to Strengthen Resilience

Ensuring Predictable Governance and Service Continuity

Article 18 of CADA would allow certain third-country providers to access assurance level 3 only if their country is designated as an “associated third country.” BSA supports cooperation with trusted partners and agrees that continuity of service, lawful access safeguards, open markets, and reciprocal treatment matter. But the current criteria are too rigid and risk excluding long-standing EU partners that are essential to Europe’s cloud, AI, cybersecurity, and semiconductor supply chains.

BSA supports an approach that enables trusted international collaboration while safeguarding continuity of service for customers that rely on globally integrated software and cloud services. Consistent with BSA’s [broader work](#) on protecting cross-border digital trade and ensuring that geopolitical measures do not unnecessarily disrupt the delivery of digital services, CADA should provide clear and predictable pathways for trusted partner countries.

Replacing the Associated Third Country Model With a Trusted Partner Framework

CADA should not treat every third-country relationship as a vulnerability, as **Europe’s resilience depends just as much on trusted partnerships as it does on domestic capability.** Instead, a distinction should be made between high-risk dependencies and cooperation with like-minded partners that share a history of strong data protection safeguards, open procurement commitments, security cooperation, and reliable channels for resolving concerns around lawful access and continuity. In particular, **Article 18 should facilitate bilateral or plurilateral frameworks under which strategic allies commit to refraining from imposing extraterritorial measures that could interrupt the provision of digital services, while benefiting from secure and reciprocal access to European markets.** Such an approach would strengthen resilience, preserve continuity of service, and support Europe’s access to innovative, secure technologies from trusted partners.

The designation process should also be transparent and predictable. **The Commission should justify any designation or refusal to designate a trusted partner,** identify the evidence relied on, and provide a mechanism for structured dialogue before market access consequences take effect. Decisions with major procurement and investment consequences should not depend on open-ended discretion.

CADA should not treat every third-country relationship as a vulnerability, as Europe’s resilience depends just as much on trusted partnerships as it does on domestic capability.

BSA Position Paper on the Cloud and AI Development Act

Sudden loss of eligibility with no access to remedies or transitional phases would increase operational risk and weaken service continuity. Accordingly, **CADA should also include transition rules**. If a third country loses its designation, providers from that country with ongoing contracts for level 3 use cases should have a realistic phaseout period, continuity safeguards for public customers, and a route to remediate specific concerns.

BSA recommends replacing the current associated third-country model with a trusted-partner approach based on objective criteria, reciprocal dialogue, and proportional safeguards. In particular, BSA finds the definition of trusted partners as *“partners that respect human rights, democratic principles and the rule of law as well as meet fundamental standards for the protection of data”* suggested by France and Germany in their recent [Joint Paper on Digital Sovereignty](#) both timely and useful. This definition would better reflect Europe’s security interests while preserving access to the partners and technologies needed to build a competitive AI ecosystem.

BSA RECOMMENDS:

- » **Replacing the “associated third country” mechanism with a broader trusted-partner approach based on objective criteria**, including respect for democratic principles, the rule of law, fundamental rights, data protection safeguards, cybersecurity cooperation, open procurement commitments, and reliable mechanisms to address lawful concerns around access and continuity;
- » Amending Article 18 to **facilitate bilateral or plurilateral frameworks under which strategic allies may commit to refraining from imposing extraterritorial measures that could interrupt the provision of digital services**, while benefiting from secure and reciprocal access to European markets;
- » **Ensuring that any refusal, suspension, or withdrawal of trusted-partner status is reasoned, proportionate, subject to review, and preceded by structured dialogue; and**
- » **Introducing transition and remediation rules** so that providers and public customers are not exposed to abrupt service disruption if a trusted partner designation changes, including reasonable phase-out periods and safeguards for ongoing public contracts.