ACCOUNTANCY EUROPE.

CONSULTATION RESPONSE

BACKGROUND

Accountancy Europe is pleased to provide below its targeted, technical recommendations to the European Commission's proposed Cloud and AI Development Act (CADA), which aims to promote sustainable cloud and AI technologies, accelerate data centre deployment and establish a Union cloud computing sovereignty framework. Our five technical suggestions aim to ensure that the proposal's assurance/audit provisions are fit for purpose and conducive to CADA's established policy objectives.

The framework comprises four Union assurance levels, with criteria set out in Annex II of the proposal. Public sector bodies would use these levels when procuring cloud computing services, based on their risk assessments:

- Level 1: data is processed and stored in infrastructure located in the Union
- Level 2: providers must demonstrate independence from third countries and transparency over their software supply chain
- Level 3: providers must be owned and controlled from the EU and meet additional criteria, such as personnel citizenship, with provision for recognised third-country providers
- Level 4: providers have full transparency and control over their software supply chain and no interference from a third country

For level 1, providers conduct a conformity self-assessment and issue a publicly available EU statement of conformity under Article 19. For levels 2, 3 or 4, providers must undergo independent third-party audits at their own expense under Article 20. To obtain recognition, they must submit the audit report, a positive audit opinion and supporting evidence to the national competent authority.

The independent audit provisions are intended to provide national competent authorities with the information needed to assess whether cloud computing services meet the applicable criteria. Our below feedback focuses on levels 2, 3 and 4 because level 1 does not require an independent third-party audit.

We would like to flag five technical issues concerning the practical operation of these provisions, possible differences in the interpretation of the assurance process and consistency with established professional assurance standards.

The reason for raising these issues is that the provisions, as proposed, appear to go against EU audit legislation and international standards, which Accountancy Europe overall supports.

FIVE TECHNICAL RECOMMENDATIONS

We propose below five technical tweaks that will ensure that CADA's audit/assurance provisions are robust and achieve the intended policy objectives.

1. AUDITOR INDEPENDENCE AND ROTATION - ARTICLE 20(4)(A)(II)

Article 20(4)(a)(ii) requires auditing organisations to:

"have not provided auditing services pursuant to this Article to the cloud computing service provider concerned or any legal person connected to that provider in the 10-year period before the beginning of the audit;"[1]

Article 20(8) states the following:

"The audited provider shall annually submit for review the audit report and the associated 'positive' audit opinion to the same or a different auditing organisation which shall assess the continued compliance of the audited service with the applicable criteria set out in Annex II. On the basis of the annual review, the auditing organisation may confirm, update, or revoke the initial audit report and audit opinion."

OUR RECOMMENDATION

Article 20(4)(a)(ii) prevents an auditing organisation from undertaking an audit if it has provided the relevant auditing services to the provider or a connected legal person during the previous ten years. Read literally, this would prevent consecutive annual engagements by the same organisation, although Article 20(8) allows annual review by the same or a different organisation. This apparent inconsistency could require a new auditing organisation each year, with no reappointment for ten years. That would disrupt continuity, require repeated familiarisation with complex cloud services and could reduce the pool of suitably qualified organisations available.

Accountancy Europe therefore proposes that Article 20(4)(a)(ii) be aligned with Article 37(3)(a)(ii) of the Digital Services Act (DSA), Regulation (EU) 2022/2065. The DSA requires independent audits of very large online platforms and search engines. Its provision limits consecutive audit appointments to ten years, allowing continuity between annual engagements.

2. TREATMENT OF PREVIOUSLY ISSUED REPORTS, ARTICLE 20(8)

We refer again to Article 20(8), quoted under point 1 above. This wording could be understood as requiring an auditing organisation to modify or reissue a report prepared for an earlier period, including a report issued by another auditing organisation. In assurance practice, however, each annual engagement assesses compliance over, or as at, a defined period and results in a report relating to that engagement.

The distinction matters because a report should tell users clearly:

- what service was assessed
- which criteria were applied
- the evaluation period or date covered
- what evidence was considered
- the conclusion reached for that date or evaluation period

Updating an earlier report could obscure these points and create uncertainty about which organisation is responsible for which conclusion.

OUR RECOMMENDATION

To avoid differing interpretations by different auditing organisations, Accountancy Europe suggests that Article 20(8) require a new assurance engagement and report for each annual cycle, while allowing relevant information from the preceding engagement to be considered.

[1] European Commission, Proposal for a Regulation establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act), COM(2026) 502 final, Articles 20(4)(a)(ii), 20(8) and 20(9), pp. 55–56.

3. SUBSEQUENTLY DISCOVERED FACTS AND REASSESSMENT, ARTICLE 23

Article 23(1) states the following:

"On becoming aware of any information or any material change in circumstances that may affect the audit report and the 'positive' opinion under Article 20 or the recognition under Article 17, the recognised cloud computing service provider shall, as soon as possible, notify the auditing organisation and the national competent authority of establishment."

And according to Article 23(2):

"On the basis of the notification under paragraph 1, the auditing organisation shall assess whether the audit report or the audit opinion need to be amended or revoked. Where the auditing organisation amends or revokes the audit report or the audit opinion, it shall, as soon as possible, notify the national competent authority of establishment."[2]

The objective in these provisions is understandable, but 'amended' and 'revoked' do not adequately describe the range of circumstances that may arise after an assurance report has been issued.

For example, new information may:

- provide evidence about circumstances that already existed when the report was issued
- relate solely to a subsequent change in the service
- be important for the audited provider's continuing recognition without changing the conclusion reached for the earlier period

These situations do not necessarily require the same response. Treating all of them as possible amendments or revocations of an earlier report could create uncertainty about the status of that report and the respective responsibilities of the audited provider, auditing organisation, and competent authority.

OUR RECOMMENDATION

The International Standard on Assurance Engagements (ISAE) 3000 (Revised), issued by the International Auditing and Assurance Standards Board (IAASB), applies to assurance engagements other than audits or reviews of historical financial information, and it expressly addresses subsequent events. Accountancy Europe recommends that the principles reflected in that standard be used as a reference point, while ensuring that CADA sets out the respective legal responsibilities clearly.

4. AUDIT EVIDENCE, ANNEX III

Article 21(1) states the following:

"To prepare the audit report and audit opinion, the auditing organisation shall assess the compliance of the audited service with the criteria set out in Annex II on the basis of the audit evidence listed in Annex III. The Commission is empowered to adopt delegated acts in accordance with Article 45 to amend Annex III by laying down the necessary evidence needed to assess the audit criteria under Annex II."

And according to Article 21(2):

"The audit evidence shall be:

[2] European Commission, proposed Cloud and AI Development Act, COM(2026) 502 final, Article 23(1)–(2), p. 57.

(a) relevant and sufficient to enable the auditing organisation to prepare an audit report and provide an audit opinion; and

(b) reliable, according to the auditing organisation's professional judgment and scepticism."[3]

Annex III would benefit from clarification that the list of evidence is illustrative rather than prescriptive. A prescriptive list may initially appear to provide greater certainty. In practice, however, the same document or evidence may not be relevant to every cloud service provider, operating model or assurance criterion. Conversely, evidence that is highly relevant in a particular engagement might not be included in a fixed legislative list.

Requiring every listed item irrespective of relevance could therefore:

- require the collection of information that is not relevant to the engagement without improving the reliability of the conclusion
- encourage a checklist-based exercise rather than a substantive assessment
- prevent the use of newer or more reliable forms of evidence as technology develops
- create an incorrect expectation that the presence of specified documents is, by itself, proof of compliance

OUR RECOMMENDATION

Accountancy Europe recommends that the auditing organisation be enabled to determine the nature and extent of evidence needed in the circumstances, applying the requirements that evidence be relevant, sufficient, and reliable. This is also consistent with the reference to professional judgement and professional scepticism in Article 21(2).

5. TIMELY ADOPTION OF DELEGATED ACT FOR THE CONDUCT OF AUDITS

Article 20(9) states the following:

"The Commission is empowered to adopt delegated acts in accordance with Article 45 to supplement this Regulation by laying down rules on the performance of audits on the procedural steps, rules for auditing organisations and their technical competences, auditing methodologies and templates for the audit reports."

OUR RECOMMENDATION

To support effective implementation, Accountancy Europe recommends that the delegated acts be adopted sufficiently in advance of the application date of the assurance requirements, potentially upon the Regulation's entry into force. This would give relevant parties adequate time to establish the necessary systems and processes, collect appropriate evidence, train personnel and put in place practical engagement arrangements, supporting a smooth and consistent transition.

[3] European Commission, proposed Cloud and AI Development Act, COM(2026) 502 final, Article 21(1)–(2), p. 56.