

Technical briefing from the European Contact Group (ECG) on the independent audit provisions in the Cloud and AI Development Act (CADA)

The ECG brings together the six largest professional services networks in Europe, providing accountancy, audit, assurance, tax and advisory services. Collectively, the firms within our networks employ more than 300,000 people across Europe in over 300 European cities. The ECG's public interest mission is to contribute constructively to European legislation and policy debates to maintain confidence in the profession and large networks in Europe.

The European Contact Group (ECG) recognises that the independent audit provisions in the proposed Cloud and AI Development Act (CADA) are intended to provide national competent authorities with the information needed to assess whether cloud computing services meet the applicable criteria for Union assurance levels 2, 3 or 4.

ECG member firms have experience of performing technical assurance engagements, including independent assurance of very large online platforms and search engines as required under the Digital Services Act (DSA). Experience under the DSA has highlighted practical challenges where common standards are not prescribed, assessment criteria are not sufficiently clear or key terms are open to different interpretations.

Drawing on this practical experience, we have reviewed the proposed assurance framework established by Articles 20 and 23 and related provisions of the proposed Regulation. Our review has identified five technical issues concerning the practical operation of certain provisions, possible differences in the interpretation of the assurance process, and terminology that is undefined or not fully consistent with established professional assurance standards¹.

Addressing these issues through targeted amendments would support consistent implementation and clear, comparable information for national competent authorities, without altering the policy objectives or overall architecture of the Commission proposal.

The five issues are:

1 Auditor independence and rotation, Article 20(4)(a)(ii)

Article 20(4)(a)(ii) provides that an auditing organisation must not have provided auditing services under the Article during the ten years preceding a new engagement. Read literally, this would appear to prevent the same organisation from carrying out consecutive annual engagements, even though Article 20(8) expressly allows the annual review to be undertaken by the same or a different auditing organisation.

This apparent inconsistency could require providers to appoint a new auditing organisation every year, followed by a ten-year exclusion period. That would disrupt continuity, require repeated familiarisation with complex cloud services, and could reduce the pool of suitably qualified organisations available to undertake the work.

We therefore suggest aligning Article 20(4)(a)(ii) with the established approach in Article 37(3)(a)(ii) of the DSA. That provision limits the duration of consecutive audit appointments and provides that an organisation must not have supplied the relevant auditing services for a period longer than ten consecutive years. This would allow reasonable continuity between annual engagements.

2 Treatment of previously issued reports, Article 20(8):

Article 20(8) requires the audited provider to submit the original report and associated 'positive' opinion for annual review by the same or a different auditing organisation. It then provides that the auditing organisation may '*confirm, update, or revoke*' the initial report and opinion.

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; and
- 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.

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

3 Timely adoption of the Delegated Act setting out rules for the conduct of audits

Article 20(9) empowers the Commission to adopt delegated acts setting out rules for the conduct of audits, including procedural requirements, criteria for auditing organisations and their technical competences, auditing methodologies, and templates for audit reports.

To support effective implementation, the delegated acts should be adopted sufficiently in advance of the application date of the assurance requirements. This would provide relevant parties with adequate time to prepare, establish the necessary systems and processes, collect appropriate evidence, train personnel, and put in place practical engagement arrangements.

In particular, consideration should therefore be given to adopting the delegated act upon the Regulation's entry into force. This would allow for an appropriate implementation period before the assurance requirements become applicable and help ensure a smooth and consistent transition.

4 Subsequently discovered facts and re-assessment, Article 23:

Article 23 requires a provider to notify the auditing organisation and the national competent authority of any information or material changes that may affect the report, the 'positive' opinion under Article 20 or

the regulatory recognition under Article 17. It then requires the auditing organisation to assess whether the report or 'positive' opinion should be amended or revoked.

The objective 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; or
- 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.

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

5 Audit evidence, Annex III

Article 21 requires the auditing organisation to assess compliance with the Annex II criteria on the basis of the evidence listed in Annex III. It also requires the evidence to be relevant, sufficient, and reliable, applying professional judgement and professional scepticism.

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 criteria. Conversely, evidence that is highly relevant in a particular engagement may 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; and
- create an incorrect expectation that the presence of specified documents is, by itself, proof of compliance.

Instead, it would be preferable to enable the auditing organisation 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).

Consistent and clearly defined terminology

We encourage the co-legislators to ensure that terminology is clearly defined and used consistently throughout Article 20, Article 23, and the relevant Annexes, with due regard to established professional standards like ISAE 3000 (Revised). Terms such as ‘audit’, ‘audit report’ and ‘audit opinion’ have recognised meanings under those standards and require clarification if a different or more specific meaning is intended under CADA.

Terms such as ‘confirm’, ‘update’ and ‘revoke’ are not established terms for describing an auditor’s response to information arising after a report has been issued by the auditing organisations. Without clear definitions, they may lead to different interpretations, inconsistent reporting, and uncertainty for competent authorities about the status of the auditor’s conclusion. We therefore encourage the use of terminology aligned with professional assurance standards (such as ISAE 3000 (Revised)) or its clear definition for the purposes of CADA.

Conclusion

These targeted clarifications would support the Commission proposal’s objectives by making the assurance framework more consistent, practicable and understandable. They would preserve strong independent scrutiny while helping competent authorities and users understand what has been assessed, the period covered and the degree of confidence that can be placed in the conclusion.

¹ *Independent assurance is a structured process in which a qualified and independent auditing organisation gathers evidence and reaches a conclusion against defined criteria. Clear criteria, appropriate evidence, and consistent terminology are therefore essential if users and authorities are to understand and rely on the conclusion. Unclear rules can produce inconsistent assessments, duplicated work, and reports that competent authorities cannot readily compare or rely on.*