european contact group

FAQ on auditing the Codes of Conduct integrated into the framework of the Digital Services Act (DSA)

Question #1: The Delegated Act does not refer to specific assurance standards, such as ISAE 3000 (Revised) Assurance Engagements Other than Audits or Reviews of Historical Financial Information ("ISAE 3000"). Would it be possible for the auditing organisation to use this (or an equivalent professional standard, such as the AICPA Attestation Standards) in conjunction with the Delegated Act, to execute and report on the VLOP's/VLOSE's compliance with the Codes of Conduct?

Answer: Yes, auditing organisations will be able to make appropriate judgments to comply with both the Delegated Act and ISAE 3000 (or an equivalent professional standard), both in terms of performance and reporting (including the template in Annex 1).

Reasons:

- The DSA, Delegated Regulation and the Codes of Conduct do not refer to specific assurance standards for the auditing organisations to follow. Article 37(3)(c) of the DSA references auditing organisations' adherence to appropriate standards, and Annex I Section 5 of the Delegated Act says that the auditing organisations should mention "any auditing standards applied in the audit, as applicable".
- Although the DSA and Delegated Regulation contain many requirements, they do not include, or incorporate by reference, all components that most assurance standards have (e.g., Quality Control aspects).
- Professional accountants traditionally perform assurance engagements in accordance with publicly available and market accepted assurance standards that have been developed with proper due process, public oversight and transparency and generally accepted internationally;
- ISAE 3000 is used by many auditing organisations for DSA audits. Since there are areas of overlap between the DSA and Commitments in the Codes of Conduct, it can also be used to audit the compliance with the Codes of Conduct.
- ISAE 3000 is commonly used globally, including in the European Union, to execute reasonable assurance engagements, when the subject matter is not historical financial information, and report on it; and is a robust assurance standard that incorporates by reference other key standards such as Independence and Quality Management.

Question #2: How does the audit provider address ambiguity in the audited provider's audited commitments?

Answer: Similar to other audits conducted under the Digital Services Act, the criteria used to assess an audited provider's compliance with Codes of Conduct includes both the specific commitments outlined in the Codes and the benchmarks the provider relies on to demonstrate compliance. As stated in Paragraph 22 of the Recitals of the Delegated Act - where ambiguity exists - "the audit criteria should be based on the information submitted by the audited provider - particularly the benchmarks used for monitoring compliance". This may also include definitions developed internally by the audited provider to support its compliance framework.

Reasons:

- Codes of Conduct may include several undefined terms. For example: 'user-friendly', 'timely', 'non-discriminatory', 'diligent' and 'without undue delay'.
- Per the Delegated Act, the audited provider should make available to the auditing organisation the benchmarks it relies upon to ensure compliance with the Code of Conduct so that the auditing organisation can base the audit criteria on this information (Paragraph 12 of the Recitals of the Delegated Act).

- The auditing organisations are expected to make comments on the audited provider's benchmarks (Article 8(1)(b)(i)).
- ISAE 3000, along with its supporting guidance, provides a structured framework for auditing organisations to assess whether the criteria used in engagements demonstrate the characteristics of suitability - namely relevance, completeness, reliability (measurability), neutrality, and understandability. It also outlines the steps auditing organisations may follow when criteria, including those mandated by law or regulation, fall short in any of these areas. In such cases, the audited provider is expected to take responsibility for establishing additional criteria to ensure suitability. Furthermore, ISAE 3000 requires that the criteria applied be made available to the intended users of the assurance report.

Question #3: Are auditing organisations performing DSA assurance engagements required to conclude on Article 45 of the DSA if the audited provider is a signatory for Codes of Conduct subject to the DSA?

Answer: No, audit organisations are not required to conclude on Article 45 of the DSA. Article 37 specifies that audited providers shall be subject, at their own expense and at least once a year, to independent audits to assess compliance with the following:

(a) the obligations set out in Chapter III;

(b) any commitments undertaken pursuant to the Codes of Conduct referred to in Articles 45 and 46 and the crisis protocols referred to in Article 48.

Articles 45, 46 and 48 within Chapter III of the DSA do not include specific obligations for the audited provider. Therefore, no conclusions are required for these Articles within the regular DSA assurance report. However, a separate opinion is required following Article 37 of the DSA for each Code of Conduct under Articles 45 and 46 to which the audited provider has subscribed and each crisis protocol under Article 48. As relevant, the auditing organisation will opine on audited provider's compliance with all relevant commitments in each code of conduct in the aggregate, as well as with each applicable individual commitment in the code of conduct.

Question #4: What is the relationship between Article 34/35 and the Codes of Conduct?

Answer: Article 34 of the DSA requires audited providers to identify and understand various risks stemming from their services. Article 35 then requires that they implement and operate reasonable, proportionate, and effective measures to mitigate any such risks. These articles are important for managing the systemic risks associated with disinformation and hate speech on digital platforms.

The Codes of Conduct, such as the Code of Conduct on Disinformation and the Code of Conduct on Countering Illegal Hate Speech Online, play a significant role in supporting Articles 34 and 35 by providing a framework for platforms to address related risks. Our understanding is that the intention for converting the Codes of Conduct under the DSA regulatory framework is to prescribe a range of measures that the audited provider may take and that may contribute to the better mitigation and management of systemic risks.

Where the risk area for a Code of Conduct overlaps with a risk area that is relevant under DSA Article 34, effectively implementing measures recommended under the relevant Code provides a positive indication that the audited provider has taken reasonable, proportionate and effective steps towards management of the relevant systemic risk.

However, Codes of Conduct are part of the mechanism by which the audited provider may manage and mitigate risks but are not the only way to manage and mitigate them. Deciding not to subscribe to a Code of Conduct (or one or more commitments/measures within a Code of Conduct where the Code of Conduct allows a more granular subscription) is a prerogative of the audited provider's management and is not deemed to indicate that the audited provider has not complied with its obligations under Article 35 of the DSA.

In respect to audit conclusions over Articles 34 and 35, a negative audit conclusion on one or more commitments in a Code of Conduct does not necessarily result in a negative audit conclusion within the DSA report. However, a negative conclusion related to a Code of Conduct is contradictory evidence of compliance with the DSA obligations. Management should demonstrate how any non-compliance with a Code may impact management's analysis of the entity's risks and its view of the

adequacy of its wider mitigation measures. The auditing organisation should also consider and evaluate whether the matter results in non-compliance with any specific DSA obligation.

Question #5: How should the audit reports on the Codes of Conduct and the DSA be presented? Should a separate audit be performed for each Code of Conduct? How should the opinions from each audit be reported?

Answer: While the DSA, Delegated Regulation, and the Codes of Conduct do not specifically discuss the required scope and presentation of the audit opinion(s) performed under Article 37 of the DSA, there are several references that refer to plural audit**s** (e.g. DSA Article 37 (1), DSA Article 37 (4), Delegated Regulation paragraph 18). Further, Article 37 (4) of the DSA states "Providers of very large online platforms and of very large online search engines shall ensure that the organisations that perform the audits establish an audit report for each audit." Based on this text, it could be concluded that separate audit reports, with separate audit opinions, should be issued for the DSA audit and the audit for each in-scope Code of Conduct. It should be noted that the Annex I to the Delegated Regulation presents the results of the audit for each Code of Conduct within the same template as the audit for compliance with the DSA.

As such, auditing organisations have the ability to issue separate audit reports for compliance with the DSA and each Code of Conduct or combine the audit reports within one (1) combined document (e.g., reporting package) including all audits performed (in alignment with Annex I to the Delegated Regulation). In all cases, the auditing organisation should issue separate opinions for compliance with the DSA and for compliance with each Code of Conduct.

Question #6: With regards to the Code of Conduct on Disinformation (hereafter the "COCD"), how will the auditing organisation evaluate and consider the underlying Measures and related Qualitative Reporting Elements (QRE) and Service Level Indicators (SLI) when forming a conclusion on the audited provider's compliance with each individual Commitment?

Answer: Audited providers may subscribe to one or more Measures for a given "Commitment" within the COCD (i.e., the COCD allows a more granular subscription below the Commitment level based on whether the Commitment and related Measures are "relevant and pertinent to the product(s), activities, and service(s) they and their subsidiaries offer"). While Article 37(1)(b) of the DSA requires an audit to assess compliance with "any commitments undertaken pursuant to Codes of Conduct…", the structure of the COCD and the ability to "commit" (i.e., subscribe) at the Measure level indicates that the signatories are committing to individual Measures (and related QREs and SLIs) of the COCD. Accordingly, for purposes of forming a conclusion, the auditing organisation should consider the subscribed Measure (and related QREs, SLIs and any relevant benchmarks) to be the commitment (as referred to in Article 37(1)(b) of the DSA) on which it provides a conclusion. The auditing organization is not responsible to evaluate or conclude on the appropriateness of the subscription selections (i.e., whether all relevant and pertinent Measures were subscribed to) as this is the responsibility of the audited provider based on the "commitments" they have undertaken pursuant to the COCD.

Therefore, the auditing organisation's assessment should evaluate compliance with the Measure subscribed to by the audited provider. Specifically, the auditing organisation should consider the following when assessing compliance with the subscribed Measures:

- For a subscribed Measure: the policies, processes, system functionalities, benchmarks, and controls designed and implemented by the audited provider. Specifically, this may include testing whether (1) the relevant policies are robust and appropriately address the related Measure, (2) the processes and/or underlying system functionalities are appropriate to support the related Measure, or (3) the controls were suitability designed, implemented and operated to effectively prevent, or detect and correct, non-compliance.
- For relevant QREs: the relevant description and disclosures reported by the audited provider in the Transparency Centre. Specifically, consideration should be given to whether the description and disclosures reported fully address the related QRE, sufficient details have been provided and the QRE accurately reflects the policies, processes, system functionalities or controls implemented based on the auditing organisation's testing of the Measure.

- For relevant SLIs: the completeness and accuracy of the data, information and metrics reported. When evaluating the SLIs, the auditing organisation should consider the relevant systems and applications and may evaluate the related IT General Controls (ITGCs) and/or controls implemented around the compilation and calculation of the data, information and metrics reported. When controls have not been implemented or evidence has not been retained to evaluate whether controls operated effectively (or if the auditing organisation determines it to be a more efficient testing strategy), the auditing organisation may take a substantive only approach to evaluating the SLIs. However, given the nature of certain SLIs and associated complexity of underlying systems, the audit provider may only be able to obtain sufficient evidence of compliance if controls are suitably designed and operating effectively.

Based on the results of the testing procedures related to the Measures, QREs and SLIs, and any necessary benchmarks defined, the auditing organisation may form a conclusion on whether the audited provider complied with the individual subscribed Measure. There may be flexibility in how the QREs, SLIs and relevant benchmarks are interpreted and designed by the audited provider and, as such, the auditing organisation will apply judgement to determine if the Measure and related QREs and SLIs, in the aggregate, are appropriately satisfied (i.e., comply with the COCD). Specifically:

- If the auditing organisation determines that the subscribed Measure, including the related QREs and SLIs were appropriately satisfied, in the aggregate, the auditing organisation may reach a “Positive” conclusion on the subscribed Measure.
- If a matter of non-compliance is identified within the Measure, or within any of the related QREs or SLIs, the auditing organisation will apply judgement and, when considering the relevant materiality threshold, determine whether the individual Measure was met (based on an aggregate assessment of compliance with the Measure and related QREs and SLIs). This includes evaluating the nature, severity, and pervasiveness of the matter, both individually and in the aggregate, to assess whether it prevents the audited provider from meeting or achieving the subscribed Measure. Ultimately, in these situations, the auditing organisation may determine if the matter results in a “Positive with comments” conclusion (i.e., the subscribed Measure is met but the auditing organisation recommends certain enhancements or improvements) or a “Negative” conclusion (i.e., there is partial or full non-compliance with the subscribed Measure).