

Mr Eric Ducoulombier
Acting Director of the Directorate-General for Financial Stability, Financial Services and
Capital Markets
European Commission

27 November 2025

Subject: Response of the CEAOB to the EC regarding DORA Article 58(3) on the review clause for statutory audits and audit firms

Dear Mr Ducoulombier,

1. The Committee of European Audit Oversight Bodies (CEAOB) wishes to thank the European Commission for consulting the CEAOB, under the review clause of Article 58(3) of the Digital Operational Resilience Act (DORA)¹, on the appropriateness of strengthened requirements for statutory auditors and audit firms as regards digital operational resilience.
2. In the accompanying technical paper, the European Commission raises six questions on which it would be interested in the views of the CEAOB.
3. As the designated body for co-operation between national competent authorities (NCAs) regarding audit oversight of the European Union and the European Economic Area, established under Article 30 of the Audit Regulation², the CEAOB hereby would like to share views on this subject, and where possible provide answers and views to the questions raised.
4. The content of this letter has been adopted by the CEAOB. It is not intended, however, to include all comments that might be provided by the individual regulators that are members of the CEAOB and their respective jurisdictions.

¹ Regulation (EU) 2022/2554.

² Regulation (EU) 537/2014.

Previous CEAOB letter on DORA proposal

5. In 2021, during the legislative process regarding DORA, the CEAOB sent a comment letter to European institutions on the DORA proposal.³
6. In that letter, the CEAOB, after having underlined the different impact on financial markets produced by cyber incidents occurring on banks or service payment systems rather than on auditors, was of the view that DORA should not automatically scope in non-financial entities such as statutory auditors and audit firms. Nevertheless, in that letter the CEAOB highlighted that, if the European legislators were to decide to further explore the need to include statutory auditors and audit firms in DORA the relevant provisions should be modified to reflect the characteristics of auditing activities and their level of ICT risks.
7. The CEAOB gave the message in that letter that proportionality should be carefully designed when recalibrating DORA's provisions to consider the size and risk profile of the different categories of auditors. For example, microenterprises are only excluded from the application of certain requirements and not scoped out of DORA. It could be worth reconsidering if the application of DORA for statutory auditors and audit firms is sufficiently proportionate in this regard.

Current CEAOB position on ICT security for statutory auditors and audit firms

8. In line with the previous letter, the CEAOB notes that while statutory auditors and audit firms contribute to financial stability through the independent opinion they provide on the financial statements of the financial entities, DORA should not automatically scope in non-financial entities such as statutory auditors and audit firms, given their different risk profile and the different role they play in the financial markets.

³ CEAOB comment letter to European institutions on the Digital Operational Resilience Act (DORA) proposal, 16 March, 2021: https://finance.ec.europa.eu/document/download/680f334c-20bc-4a75-a619-70c1ccb2962_en?filename=210316-ceaob-comment-letter-dora_en.pdf.



9. At the same time, the CEAOB acknowledges that the growing use of technology in auditing will probably make it necessary to reinforce the current requirements on ICT security set out in the Audit Directive.⁴
10. The current Article 24a of the Audit Directive⁵, dealing with the internal organisation of audit firms, states general overarching principles requiring auditors and audit firms to have effective control and safeguards arrangements on information processing systems and incidents that could impact the integrity of the statutory auditors' and audit firms' activities. Those general provisions do not, however, explicitly focus on information technology (IT) systems and information and communication technology (ICT) risks.
11. Following your request of 16 September, the CEAOB has sent out a survey among its members to gather their views. It should be noted that some of your questions touch upon topics that would have required more time for NCAs to carry out specific and detailed work in order to collect the information necessary to answer your questions.
12. This survey and following interactions show that the CEAOB generally still supports the messages from the 2021 letter, particularly those mentioned in paragraphs 6 and 7 above.
13. The observations of the CEAOB confirm that the use of ICT, including the use of artificial intelligence (AI), by audit firms in auditing and in contact with their audit clients has continued to grow since 2021. Especially since the COVID-pandemic, when multi- and hybrid-cloud solutions, remote access interfaces

⁴ Directive 2006/43/EC.

⁵ Article 24a of the Audit Directive:

"1. Member States shall ensure that a statutory auditor or an audit firm complies with the following organisational requirements:

[...]

b) statutory auditor or an audit firm shall have sound administrative and accounting procedures, internal quality control mechanisms, effective procedures for risk assessment, and effective control and safeguard arrangements for information processing systems.

[...]

i) a statutory auditor or an audit firm shall also establish appropriate and effective organisational and administrative arrangements for dealing with and recording incidents which have, or may have, serious consequences for the integrity of his, her or its statutory audit activities;"



and supply chain interconnectivity⁶ gained significant momentum and created a higher digital dependency.

14. Relatedly, the European Union Agency for Cybersecurity (ENISA) describes the cyber threat ecosystem as a maturing threat environment.⁷
15. The CEOB is of the opinion that ICT security at audit firms is an important organisational requirement for a sound performance of the audit engagements. Because of the importance of this security, a majority of the members of the CEOB believes that strengthened requirements are needed around this security.
16. Statutory auditors and audit firms are important actors in the financial sector. By providing services such as statutory audits to all other actors in the financial sector, they have privileged access to highly sensitive information of their clients.
17. On the one hand, audit firms often establish long-term remote access interfaces with audited entities in order to extract data to feed remote (often third-party) audit tools. On the other hand, they usually extract significant volumes of sensitive controls, transactional and personal data from audited entities to execute their audit work. Additionally, there is IT dependency and concentration risk due to reliance on a limited number of cloud and third-party audit software providers. In the financial sector this dependency amplifies the risk of disruption.⁸ Due to growing digital interconnectivity, statutory auditors and audit firms are targets for cybercrime (e.g. ransomware, island-hopping and widening the supply chain attack surface). Breaches of remote network access interfaces or the confidentiality of the information stored by audit firms may have adverse impacts on the financial markets and could potentially lower confidence in the financial system.

⁶ Also driven by the implementation of the EU e-invoicing Directive (2014/55/EU) in conjunction with the EU VAT Directive and "VAT in the Digital Age" (ViDA) legislation.

⁷ ENISA Threat Landscape 2025, 1 October 2025: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>.

⁸ AFM and DNB publication: AFM and DNB warn of systemic risks in the financial sector from digital dependence, 20 October 2025: <https://www.afm.nl/en/sector/actueel/2025/okt/pb-digitale-autonomie>





18. The Audit Directive requires that auditors and audit firms apply general rules of confidentiality professional secrecy (Article 23(1)) and effective control and safeguard arrangements for information processing systems (Article 24a(1)(b)) and incidents (Article 24a(1)(i)) as already mentioned in paragraph 10. Those relevant provisions apply without additional specificity on the minimal protection that needs to be put in place on ICT.
19. To complement the current general rules in the Audit Directive, the CEAOB has considered two potential directions to strengthen the ICT security at audit firms: (1) amending the Audit Directive and Audit Regulation (2) re-assessing the scope of DORA, in order to include statutory auditors and audit firms, taking into account their specificities. The CEAOB recognises that both pathways identified in the review clause in Article 58(3) of DORA could result in enhanced ICT security measures, which have different pros and cons that need to be taken into account.

CEAOB's views on the questions of the European Commission

20. Regarding the review clause, the Commission is seeking CEAOB's views on whether statutory auditors and audit firms should be subject to strengthened requirements via the questions stated in the table below.

Commission's request	CEAOB Response
-----------------------------	-----------------------

Question 1: What are the risks, challenges and gaps in relation to the digital operational resilience of audit firms within the EU?

- Risks: Data sensitivity and confidentiality, Dependence on ICT and cloud systems and (AI-)tools, (Global) network reliance, Third-party reliance, Market access and reputation, risk of concentration.
- Challenges: Resource disparities, Managing data access, Incident reporting and transparency: Governance and awareness, Translating regulatory expectations into practice, Embedding digital operational resilience into quality management.
- Gaps: Despite their important role in safeguarding trust in financial reporting, audit firms are not integrated into the EU's operational resilience framework, resulting in limited alignment with financial stability mechanisms..

Question 2: Do audit oversight bodies have the resources and skills needed to perform the oversight/supervision of audit firms on DORA? Is there any analysis of the impact on resources that

Audit oversight bodies already possess expertise in supervising statutory audits including IT-related aspects. However, their focus has traditionally been on audit quality, independence and compliance with auditing standards. Skills in areas such as cybersecurity, ICT resilience testing and critical third-party risk assessment would probably require additional expertise in NCAs.





Commission's request **CEAOB Response**

DORA implementation might trigger?

DORA implementation would likely require additional investment in staff training, hiring of ICT/cybersecurity experts and development of technical supervisory tools.

No analysis of impact on resources (in terms of competence and workload) has been performed at CEOAB level, as the outcomes would be dependent on the scope and proportionality of the requirements and population covered. Data on the audit market participants is available in the market monitoring reports drawn up under Article 27 of the Audit Regulation.

Question 3: How is the ICT risk management function implemented by audit firms?

Audit firms generally implement ICT risk management as part of their internal governance, drawing on the requirements of the Audit Directive and international standards, such as the International Standards on Quality Management 1 (ISQM 1).⁹

Larger audit firms and international audit networks have established dedicated IT governance structures with policies covering cybersecurity, data protection, business continuity and incident management. ICT risk management is often embedded in their global risk management frameworks including risk assessment, controls, monitoring and reporting.

The maturity of ICT risk management can vary significantly between audit practices, where the size of the firm (associated with the number of internal resources in the firm that share IT tools) can play a role. This size may also play a role in the level of internal resources that may be dedicated in the implementation of advanced cybersecurity controls and structured ICT governance.

Question 4: How many cyber-attacks do audit firms face on average every year? Are they subject to ICT and security incident reporting requirements?

There is no publicly available statistical data on the average number of cyber-attacks audit firms face each year. However, given their role as holders and processors of highly sensitive financial and client data, audit firms, and particularly audit firms that are part of international networks, are considered prime targets for malicious actors.

International standards such as ISQM 1 encourage documentation and follow-up of security incidents. However, these requirements are internal to the firms and do not imply reporting to national audit oversight bodies or other competent authorities. Moreover, not all Member States have incorporated ISQM 1 into their regulatory framework.

Question 5: Do audit firms perform any ICT and security testing/assessment of their ICT systems and tools (e.g. gap analyses, vulnerability scans, threat led penetration testing, etc.)?

International audit networks carry out a range of ICT and security assessments as part of their global risk management and compliance frameworks. These may include:

- vulnerability scans and patch management reviews to identify weaknesses in their systems,
- penetration testing conducted by internal cybersecurity teams or external providers,
- business continuity and disaster recovery testing to assess resilience against operational disruptions.

⁹ ISQM 1 requires audit firms to implement responses to address quality risks, which includes risks related to IT/ICT resources.





Commission's request **CEAOB Response**

Many audit firms also maintain certifications (e.g. ISO 27001) that require periodic independent audits of information security management systems. The investments by the networks and audit firms range from structured ICT testing programs, to more basic assessments and, by exception, rarely no formal IT governance in place.

Question 6: How do audit firms assess and manage third-party risk, particularly when relying on external service providers for outsourced functions?

Audit firms and their international networks often rely on external service providers for IT infrastructure, cloud services, data storage, software solutions and in some cases for support functions. As part of their governance frameworks, they generally implement policies and procedures to assess, monitor and manage third-party risks. Typical assessment practices include:

- collecting provider's certifications such as ISO 27001 or SOC reports,
- reviewing audit reports covering areas such as business continuity, access rights management and data confidentiality,
- monitoring performance against contractual obligations, for example through service level agreements (SLAs).

21. To conclude on the above analysis, the CEOB observes that audit firms are not directly connected to the digital operational resilience of financial entities or to the overall stability of the financial system. Nevertheless, the CEOB believes that the operational resilience of auditors and audit firms needs to be strengthened with a proportionate and risk-based approach.,

Proportionality is essential

22. If the digital operational resilience requirements for statutory auditors and audit firms were to be increased, proportionality should be considered in both cases, either strengthening the Audit Directive and Regulation or by including statutory auditors and audit firms in the scope of DORA.

23. Should the Audit Directive and Regulation route or the DORA route be taken to strengthen the requirements on ICT security, the provisions applicable to statutory auditors and audit firms would have to be carefully designed to consider the specific risk profile related to the audit activity as well as the size and risk profile of the different categories of auditors in a proportionate way. This approach would be in line with the European Commission's goal of simplification and burden reduction, to prevent overly burdensome and costly requirements for some categories of statutory auditors and audit firms. Otherwise, some statutory auditors and audit firms may decide to exit the



market to avoid its implementation. This would be in contradiction with the stated objective of the EU Audit reform of 2014 to contribute to more dynamic audit market in the EU.

24. The CEAOB believes that a balanced scope should be worked out to capture the audit firms with audit clients that are themselves in the scope of DORA (i.e. financial firms).

Cost/benefit analysis to identify pros and cons of the possible paths

25. However, the CEAOB believes that the two alternative directions identified above have different pros and cons and require an adequate cost/benefit analysis, which also takes into consideration the administrative burden and the additional expertise NCAs need to attract. In this context it is also important to underline that strengthening the Audit Directive and Regulation would allow to build up on the already existing audit oversight framework and thereby tailor appropriate rules in coherence with that. The benefits should be assessed versus the inclusion of statutory auditors and audit firms in the scope of DORA, which is set up in the context of the financial entities' framework.

Role of the CEAOB under the DORA route

26. We would like to re-iterate our observation from 2021 that should the DORA route be chosen to strengthen the requirements for statutory auditors and audit firms as regards digital operational resilience, some coordination of oversight and Regulatory Technical Standards would be elevated to the European level, whereby the European Supervisory Authorities would play a major role. We observe that none of the existent European Supervisory Authorities (ESAs) has a mandate or specific expertise regarding audit oversight, and hence we would advise that the CEAOB be involved in any future work aimed at designing a framework for audit firms. The CEAOB has currently not the powers and the structure of an ESA and its involvement could raise a number of issues to take into account.



Conclusion

27. In conclusion, the CEAOB believes that ICT security for statutory auditors and audit firms is an important organisational requirement. Therefore, a majority of the members of the CEAOB are of the opinion that strengthened requirements are needed on ICT security (and AI), given the increased risk landscape resulting from growing digital interconnectedness and the associated cyber risk threats to the financial sector. However, as DORA is aimed at improving operational digital resilience of financial entities, the requirements under DORA are not all relevant or suitable for statutory auditors and audit firms, which would make it necessary to modify and tailor the DORA provisions in order to apply them to auditors. Therefore, the CEAOB is of the opinion that the best route to strengthen the requirements regarding ICT security for statutory auditors and audit firms would be to complement the Audit Directive and Regulation, as it would make it easier to tailor appropriate and proportionate requirements, taking into account the specificities of statutory auditors and audit firms. Overarching, the CEAOB believes the strengthening of ICT requirements for statutory auditors and audit firms should follow a thorough impact analysis that considers all the elements indicated above.

We remain at your disposal, should you need any clarification or wish to discuss our views in greater detail.

Yours faithfully,

Panos Prodromides

Chairman

