COMMITTEE OF EUROPEAN AUDITING OVERSIGHT BODIES

Irene Tinagli MEP
Chair of the Committee on Economic and Monetary Affairs (ECON)
European Parliament

Joao Leão
President of the ECOFIN Council
Council of the European Union

Mairead McGuinness
Commissioner in charge of Financial stability, financial services and Capital Markets Union
European Commission

16 March 2021

Subject: Proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector

Dear Ms Tinagli, dear Mr Leão, dear Ms McGuinness,

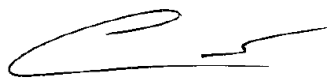
1. We are pleased to share the views of the Committee of European Auditing Oversight Bodies (CEAOB) on the European Commission's proposal for a regulation on digital operational resilience for the financial sector ("DORA").
2. As the organisation representing the audit regulators of the European Union and the European Economic Area, the CEAOB encourages and supports continuing improvements in high quality auditing through the development of professional standards for the audit profession.
3. The content of this letter has been prepared by the International Auditing Standards Subgroup and has been adopted by the CEAOB. The comments raised in the letter reflect matters agreed within 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.
4. The proposal for regulation DORA states that new technologies are transforming the EU financial system and the way it provides services to Europe's businesses and citizens. It also considers that digital operational resilience and security are critical for highly digitalised and interconnected financial institutions to ensure business continuity and the provision of high-quality services to consumers.

5. The CEAOB acknowledges the general objective, which is behind the DORA proposals to further enhance the resilience of the financial sector to maintain market integrity and financial stability while appropriately tailoring these proposals to the specific characteristics of the entities to which they would apply.
6. The CEAOB notes that statutory auditors and audit firms are labelled financial entities in the proposed regulation, even if they do not provide directly "financial services" and contribute to financial stability through the independent opinion they provide on the financial statements of the financial entities. We agree that as for every entity, whether in the financial sector or outside, statutory auditors and audit firms need to reduce and manage Information Communication and Technology (ICT) risks to ensure the continuity of their activities in case of cyberattack.
7. Protection of data, including data received from clients for the purpose of the audit, is also a key element that deserves increased care and security, and that will become even more central in the context of the growing use of technology (including data analytics) in auditing.
8. Moreover, as for any other entity, it is also important for statutory auditors and audit firms to avoid that any operational incidents encountered in their internal systems may spread to their clients.
9. The need for control in those three areas has indeed been acknowledged by Article 24a 1(b) of the Directive 2006/43/EC (as revised by Directive 2014/56/EC) which requests statutory auditors and audit firms to have in place effective controls and safeguard arrangements for information processing systems.
10. DORA is proposing a robust framework to ensure digital operational resilience for financial entities. It is also possible that DORA may be a point of reference in the future for similar legislation for entities outside the financial sector.
11. While a cyber-attack on a bank or service payment system ICT resulting in that entity being unable to serve its clients is a risk that has so far-reaching consequences so that a robust framework such as DORA is clearly a "must have", the CEAOB is not convinced that the same is true for statutory auditors and audit firms. If their ability to serve their clients is interrupted during 24, 48 or 72 hours, it will not likely result in a systemic risk.
12. Therefore, the CEAOB considers that DORA should not automatically scope in non-financial entities such as statutory auditors and audit firms.
13. On the other hand, as noted above, the CEAOB acknowledges that the growing use of technology in auditing will probably make it necessary to reinforce the current requirements set out in the Directive 2006/43/EC (as revised by Directive 2014/56/EC). If in this light, the European legislators were to decide to further explore the need to include statutory auditors and audit firms in DORA, we believe that DORA's provisions should be modified to reflect the characteristics of auditing activities and their level of ICT risks.
14. In this case, proportionality would have to 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 is sufficiently proportionate in this regard.

15. Moreover, the criteria set out to qualify for microenterprises may not have the intended effect when applied to statutory auditors and audit firms. For example, sole audit practitioners might not qualify for microenterprises as they are individuals. As such, a sole practitioner would have to apply DORA in the same way a large bank, except for some requirements. A firm with a very small ("micro") audit activity but providing other types of consulting or expert services will easily reach the threshold of more than 10 employees, which is not uncommon in these labour-intensive activities, and so would be outside the "microenterprise" exemption.
16. More generally, the scope of DORA should be reviewed 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 of the stated objective of the EU Audit reform of 2014 to contribute to more dynamic audit market in the EU.
17. As currently drafted, all statutory auditors and audit firms will be required in general to apply the same provisions as large financial institutions, even if they do not have any clients in the financial sector. This will go beyond what is necessary to meet the objectives of this initiative. We believe that a balanced and efficient scope could be worked out to capture only those audit firms with audit clients that are public interest entities in the scope of DORA that meet specific criteria (based on the characteristics of the business or on the size of those audit clients).
18. We also observe that based on DORA, some coordination of oversight and Regulatory Technical Standards will be elevated to European level, whereby the European Supervisory Authorities will play a major role. We observe that none of the extant ESAs has a mandate nor specific expertise regarding audit oversight, and hence we would advise that the CEAOB be involved in future work aimed at designing the DORA framework for audit firms.
19. In all cases, we believe that the regulation should strike the right balance between a protective level of digital resilience as well as the appropriate level of proportionality that will allow smaller and medium size audit firms to serve public interest entities even in the financial sector: our proposals are meant to address both objectives simultaneously.

We remain at your disposal to provide any clarification and to discuss our concerns in greater detail.

Yours faithfully,



Patrick Parent

Chairman