ACCOUNTANCY EUROPE.

Mr. John Berrigan,
Director-General DG FISMA

Cc:
Mr. Jan Ceyssens, Head of Unit B5 Digital Finance
Mr. Mattias Levin, Deputy Head of Unit B5 Digital Finance

Submitted via website and email

Brussels, 16 December 2020

Subject: Response to the European Commission's proposed regulation concerning digital operational resilience for the financial sector

Dear Mr. Berrigan,

We are pleased to share our views on the European Commission's (EC) proposed regulation concerning digital operational resilience for the financial sector, also known as the Digital Operational Resilience Act (DORA).

(1) Accountancy Europe welcomes the EC's digital finance package, which we believe supports the European Union (EU)'s ambition for a recovery by means of a digital transition.

(2) The accounting and audit profession ('the Profession') supports the important EU digital agenda and believes that digitalisation could be a catalyst to modernise the European economy across sectors and turn Europe into a global digital player.

(3) Accountancy Europe is committed to contribute to the EC's digital finance package. Regarding in particular the proposed DORA and the inclusion of statutory auditors and audit firms in its scope, we would like to express the following concerns.

Scope and application of the 'proportionality' principle in a DORA context

(4) The proposed regulation applies to a wide range of financial sector entities, covering 20 types of financial entities regulated at EU level. Statutory auditors[1] and audit firms[2] ('Auditors') are also considered as financial entities in the context of this legislation (Article 2 (q)), although in essence and in practice, Auditors are not "financial entities" per se despite the important role they play in the financial sector. As a result, it is proposed in the regulation that Auditors as such have to comply with the same requirements as e.g. banks.

[1] 'statutory auditor' means statutory auditor as defined in point (2) of Article 2 of Directive 2006/43/EC
[2] 'audit firm' means an audit firm as defined in point (3) of Article 2 of Directive 2006/43/EC

(5) The application of the 'proportionality' principle in a DORA context is reflected in two ways throughout the proposed regulation.

(6) Firstly, a lighter regime is proposed for microenterprises[3]. Secondly, proportionality is embedded in the proposal either through tailored rules for certain categories (e.g. advanced digital resilience testing is only applicable for *significant* financial entities) or for certain aspects (e.g. ICT-related incident reporting is only applicable in case of *major* ICT-related incidents). We believe that the application of the 'proportionality' principle has not been fully developed yet in the context of DORA, and especially is not calibrated for Auditors.

(7) The inclusion of Auditors in the scope of DORA and the operation of the proportionality principle in their case should be based on an impact assessment looking at (i) the cost/benefit of the inclusion of Auditors in view of fulfilling the purpose of DORA and (ii) whether other regulations or standards are already contributing to the purpose of DORA concerning Auditors.

(8) We therefore believe that further engagement between the European institutions and the Profession would help ensuring the relevance and effectiveness of the scope and the operationalisation of the 'proportionality' concept in the proposed regulation.

DORA scope & Auditors – Considerations

(9) The regulation acknowledges that significant differences exist between financial entities in terms of size, business profiles or in relation to their exposure to digital risk. We also note the following general principle in the proposed regulation[4]: When directing resources and capabilities to the implementation of the ICT risk management framework, financial entities should duly balance their ICT-related needs to their size and business profile, while competent authorities should continue to assess and review the approach of such distribution.

(10) Auditors solely use IT as a tool to perform audits on a sample and 'as needed' basis as part of their internal processes. The use of data, in the context of an audit, is mainly limited to the audited company's historical transaction data. The Auditor's IT systems furthermore do not create an IT gateway to access the company's information nor act as a back-up of the company's data or systems. The use of IT by Auditors is as such not critical for the daily operation nor the digital resilience of the financial markets.

(11) The provisions of the proposed EC regulation are aimed at core financial service providers who use transactional systems, relying on highly automated ICT systems, in providing financial services to the market (e.g. online banking, payment transactions etc.). The ICT and related security risks faced by these financial sector entities can indeed entail important risks to financial stability. Therefore, they need robust systems as they are often targeted by cybercrime attacks.

(12) However, Auditors have no transactional systems that have to perform 24/7 as part of their business model.

a. Auditors issue audit reports based on the performed audits of clients. They are service providers to their clients, active in financial services or other sectors. Auditors have no direct involvement with the activities or processes of their clients. Their indirect involvement is limited to providing assurance on client's financial statements and other assurance services required by laws and regulation.

b. The work of Auditors results in a written document that makes a qualitative professional assessment of whether the accounts of their clients represent a 'true and fair' view of

[3] 'microenterprise' means a financial entity as defined in Article 2(3) of the Annex to Recommendation 2003/361/EC
[4] Recital 33 of DORA

the underlying activities. Auditors must exercise independent judgment in the performance of their professional activity and do not rely on automated ICT systems in this context. The Auditor's ICT environment is as such not so complex compared to financial entities (e.g. banks).

c. The sources of risk for the Auditor's activities are not primarily their ICT systems, but are instead mainly related to the principles of independence and professional scepticism. These audit-related risks are already regulated. Recent legislation at EU level, i.e. the 2014 Audit Regulation and amendments to the Audit Directive, have harmonized the regulatory framework and made it more stringent.

(13) Auditors are already subject to oversight and regulation concerning the resilience of their ICT systems, including the following provisions in the Audit Directive and by the International Standard on Quality Management (ISQM) 1[5]:

a. Requirement to have a business continuity policy that requires them to use appropriate systems, resources and procedures to ensure continuity and regularity in the carrying out of his, her or its statutory audit activities[6].

b. ICT-related incident reporting obligations that require them to 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[7].

c. The business of audit firms in terms of organisation and processes are covered by the ISQM 1 rules, which also covers IT-processes. The rules stipulated in ISQM 1 require significant risk management, controls, documentation and follow-up etc. The Auditor's compliance with these rules is subject to supervision by the national competent authority.

(14) Auditors do not provide financial services and are not subject to the supervision by the European Supervisory Authorities (ESAs).

(15) Auditors' services are provided to a wide range of types of entities engaging in different types of economic activities, not just financial services' firms.

Our recommendation to the EC

(16) In the light of the above considerations, Accountancy Europe would like to propose the following: Firstly, we would see a lot of value for the EC to perform a cost/benefit analysis of scoping in Auditors in the proposed regulation in the context of its impact assessment exercise. Secondly, it would be helpful to understand why Auditors are scoped in and whether the proposed scope has captured entities faced with significant ICT risks.

(17) As highlighted above, Auditors provide services to a wide range of entities. Should the EC conclude that Auditors need to be included in the scope, it would be important to reflect as to (i) whether all Auditors should be included considering that the majority of Auditors are not involved at all in the financial sector and (ii) how proportionality should apply to them so that DORA applies to Auditors in a manner proportional to their activities (financial/ non-financial sector), size and resources. On this basis, provided the need for Auditors to be involved to attain the objectives of DORA is established, and taking into account all the above clarifications on the measures already in place, we believe that

[5] ISQM 1 will replace the International Standard on Quality Control (ISQC) 1 in 2022 as issued by the International Audit and Assurance Standards Board (IAASB) upon Public Interest Oversight Board (PIOB) approval.
[6] Article 24(a)(1)(h) of the Directive 2014/56/EC
[7] Article 24(a)(1)(i) of the Directive 2014/56/EC

only Auditors who audit core financial service providers that fall in the scope of DORA should be concerned (i.e. Auditors of banks and insurance companies). This suggestion would also still be consistent with the EC's intention to have a broad scope of the proposed regulation to capture in a comprehensive way all actors in the financial ecosystem to ensure digital operational resilience of the interconnected players.

(18) Additionally if DORA were to include Auditors in its scope, even if it is limited to Auditors of financial entities which are within the scope of DORA, the legislation should be adapted for the Auditors before including them. Otherwise, there is a great risk that the legislation be designed for financial entities and unsuited for Auditors. We have seen examples of that with the Anti-Money Laundering directives which were primarily written for banks and contain requirements which are not adapted to the nature of the auditor's engagement.

We hope the above is of help to the EC in defining the most appropriate and effective scope for DORA. Please do not hesitate to contact Ben Renier (ben@accountancyeurope.eu) in case of any additional questions or remarks.

Sincerely,

Florin Toma
President

Olivier Boutellis-Taft
Chief Executive

ABOUT ACCOUNTANCY EUROPE

Accountancy Europe unites 51 professional organisations from 35 countries that represent close to **1 million** professional accountants, auditors and advisors. They make numbers work for people. Accountancy Europe translates their daily experience to inform the public policy debate in Europe and beyond.Accountancy Europe is in the EU Transparency Register (No 4713568401-18).