

18 January 2021

Mr. John Berrigan  
Director-General DG FISMA

Cc:

Mr. Jan Ceyskens, Head of Unit B5 Digital Finance  
Mr. Matthias Levin, Deputy Head of Unit B5 Digital Finance

submitted electronically via the European Commission website

Institut der Wirtschaftsprüfer  
in Deutschland e.V.

Wirtschaftsprüferhaus  
Tersteegenstraße 14  
40474 Düsseldorf  
Postfach 32 05 80  
40420 Düsseldorf

TELEFONZENTRALE:  
+49 (0) 211 / 45 61 - 0

FAX GESCHÄFTSLEITUNG:  
+49 (0) 211 / 4 54 10 97

INTERNET:  
[www.idw.de](http://www.idw.de)

E-MAIL:  
[info@idw.de](mailto:info@idw.de)

BANKVERBINDUNG:  
Deutsche Bank AG Düsseldorf  
IBAN: DE53 3007 0010 0748 0213 00  
BIC: DEUTDE33XXX  
USt-ID Nummer: DE119353203

## **Re.: Response to the European Commission's proposed Digital Operational Resilience Act concerning the financial sector**

Dear Mr. Berrigan,

The Institut der Wirtschaftsprüfer in Deutschland e.V. [Institute of Public Auditors in Germany, Incorporated Association] (IDW) appreciates the opportunity to provide its views on the European Commission's (EC) proposed Digital Operational Resilience Act (DORA), i.e. the "Proposal for a regulation on digital operational resilience for the financial sector and amending Regulations (EC) No [...]" and the "Proposal for a directive amending Directives 2006/43/EC, [...]".

The IDW represents approximately 12,000 Wirtschaftsprüfer [German Public Auditors], which is over 80 % of all Wirtschaftsprüfer in Germany. Our members are from the only profession in Germany to have been entrusted with the performance of statutory audits of the financial statements of larger companies and Public Interest Entities.

As an association representing German Public Auditors our comments on DORA are focused on issues concerning statutory auditors and audit firms.

### **General comments**

We support the EC's objective, set out in the recitals of the proposed regulation, to strengthen the operational resilience of digital systems in the financial sector in order to counter the possible detrimental impacts of cyberattacks on financial entities and their customers as well as on the stability of the European Union's

GESCHÄFTSFÜHRENDER VORSTAND:  
Prof. Dr. Klaus-Peter Naumann,  
WP StB, Sprecher des Vorstands;  
Dr. Daniela Kelm, RA LL.M.;  
Melanie Sack, WP StB

**Page 2 of 4** to the Comment Letter to the European Commission of 18 January 2021

financial system. Providing assurance services in relation to risk management and compliance systems is already one of the core activities undertaken by auditors and audit firms, whether required by law, as is the case in various industries, or on a voluntary basis. The auditing profession in Germany is ready to support companies who, in future, will fall within the scope of the regulation. Such support could be in the form of advisory services as companies establish an ICT risk management system to counter cyber threats, or by providing assurance services regarding the effective operation of such systems. In this way the profession can make a significant contribution to achieving the objectives associated with the proposed legislation.

### **Personal scope of the proposed regulation**

The planned inclusion of statutory auditors and audit firms within the meaning of Article 2 No. 2 and No. 3 of the Directive 2006/43/EC (Audit Directive) in the scope of the proposed regulation (Article 2 No. 1 (q)) triggers considerable concerns. In essence, the proposed scope would include every statutory auditor or audit firm carrying out a statutory audit (e.g. also of a medium-sized limited liability company). Auditors and audit firms, however, are not generally subject to the same ICT risks that we understand to be addressed by the proposed regulation, because they have no direct involvement in the activities or processes of their (financial sector) clients, e.g., they neither manage payment solutions nor execute securities transactions nor are they required to operate any other comparable transactional system(s) 24/7 as part of their business model. In our view, auditors' ICT systems do not constitute critical systems in terms of any role in maintaining the operations of companies in the financial sector and in terms of ensuring the resilience of the entire European financial system against cyberattacks. The auditor also does not act as a back-up support mechanism for companies' financial data. These aspects also all apply equally to auditors of credit institutions, insurance undertaking or other "financial entities" within the scope of the draft regulation.

Given the above, we suggest the deletion of Article 2 No. 1 (q) of the proposed regulation.

### **Proposed amendment of the Audit Directive**

For the reasons stated above, we also reject the proposed amendment to the Audit Directive, according to which statutory auditors and audit firms would, in future, have to comply with the requirements of Article 6 of the proposed regulation (amendment of Article 24a (1) (b) Audit Directive). The Audit Directive already contains requirements concerning statutory auditors' and audit firms'

**Page 3 of 4** to the Comment Letter to the European Commission of 18 January 2021

data processing systems. These requirements are implemented by the respective auditing practice, bearing in mind the respective scope of the firm's activities and range of clients, and has proven to be effective. Extant Article 24a (1) (b) of the Audit Directive stipulates, among other things, that statutory auditors and audit firms must have effective control and safeguard arrangements for information processing systems. This includes, in particular, procedures to ensure the confidentiality, integrity and availability of the systems, including regulations on access rights. In addition, Article 24a (1) (i) of the Audit Directive requires statutory auditors and audit firms to establish appropriate and effective organisational and administrative arrangements for dealing with and recording incidents which have, or may have, serious consequence for the integrity of the audit activities. The relevant professional standards, in particular ISQC 1 (International Standard on Quality Control), also define requirements in this regard (see ISQC 1, para. 46). Compliance with the above-mentioned requirements is also subject to professional supervision by the competent authority.

We therefore fail to see any need for the proposed amendment to the Audit Directive, according to which statutory auditors and audit firms would in future also have to comply with the requirements of Article 6 of the proposed DORA regulation. If the proposed amendments were to be implemented, the ICT systems of statutory auditors and audit firms would also have to meet requirements aimed at managing risks in highly automated processes, i.e. there would, for example, have to be sufficient capacity to deal with "peak orders, message or transaction volumes" (Article 6 no. 1 lit. (c) of the proposed regulation) and be "resilient to adequately deal with additional information processing needs as required under stressed market conditions" (Article 6 No. 1 lit. (d) of the proposed regulation). This appears neither necessary nor reasonable, since statutory auditors and audit firms, as explained above, neither have a direct part in the operational processes within the financial sector nor are their ICT systems subject to the risks addressed by DORA.

We therefore suggest the proposed amendment to the Audit Directive to be deleted.

### **Compatibility with the principle of proportionality and the Audit Reform's objectives**

For the reasons set out above, both the inclusion of statutory auditors and audit firms within the scope of the proposed regulation and the proposed amendment to the Audit Directive go well beyond what is necessary to achieve DORA's objectives. They are therefore incompatible with the principle of proportionality.

**Page 4 of 4** to the Comment Letter to the European Commission of 18 January 2021

Should the Commission nevertheless intend to include, as a minimum, the statutory auditors of credit institutions, insurance undertakings and possibly other financial entities within the scope of the proposed regulation, we believe that in accordance with the principle of proportionality significant adjustments to the requirements would be urgently needed, in order to take into account the completely different function of the respective auditors' ICT systems compared to the ICT systems applicable to the audited financial entities.

Furthermore, it is already apparent that the most recent comprehensive audit reform, leading to Regulation (EU) No 537/2014, which has been in force since 2016, has led to increased market concentration, especially in regard to the audit of public interest entities. This is contrary to the political intention. The approach of the proposed rules - the transfer of regulatory requirements applicable to companies in certain sectors to the entire audit profession or to auditors of these companies - would introduce additional and considerable burdens for statutory auditors and audit firms, although the proposed regulation indeed excludes parts of the catalog of requirements for so-called "microenterprises". As a result, it would very likely only be feasible for auditors and audit firms to participate in the statutory audit market if they perform a large number of statutory audits. This would cause a further withdrawal of small and medium-sized auditing practices from the statutory audit market. Taking this into account also, we urge the Commission to limit the scope of the proposed regulation to companies within the financial sector, to which statutory auditors and audit firms do not belong.

We would be pleased to provide you with further information if you have any additional questions about our response, and would be pleased to be able to discuss our views with you.

Yours sincerely

Prof. Dr. Klaus-Peter Naumann  
Chief Executive Officer