INSTITUT DER WIRTSCHAFTSPRÜFER

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

E-MAIL:
info@idw.de

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

2 February 2021

Mr. Eric Vetillard
Lead Certification Expert, ENISA

submitted electronically via E-Mail

Re.: Response to the ENISA's draft EUCS – Cloud Services Scheme (a candidate cybersecurity certification scheme for cloud services)

Dear Mr. Vetillard,

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 ENISA's draft EUCS – Cloud Services Scheme (a candidate cybersecurity certification scheme for cloud services).

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.

Our association represents German Public Auditors, but we strongly believe that our comments on EUCS pertain to all Public Auditors in the EU.

General comments

We support the aims of the draft EUCS scheme mentioned under 3. PURPOSE OF THE SCHEME to enhance the level of security for a wide range of cloud services, the cloud capabilities they implement, including application, infrastructure, and platform capabilities.

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 is ready to support cloud service providers who, in future, want to be certified under the requirements set forth in the EUCS scheme. In this way the audit profession can make a significant contribution to achieving the objectives associated with the draft EUCS scheme.

Accreditation process

As set out under 7. SPECIFIC REQUIREMENTS APPLICABLE TO A CAB in the draft EUCS scheme, all conformity assessment bodies (CABs) performing assessments in the context of the EUCS scheme will need to be accredited for under the ISO 17065 standard.

The nature and extent of the accreditation and other quality maintenance processes that the audit profession is already subject to makes an additional accreditation process not only redundant, but reflects an additional effort and cost that is unnecessary in the circumstances.

Due to the fact, that the audit profession is obliged to conduct assurance engagements based on the IAASB's Assurance standards and the IESBA's Code of Ethics for Professional Accountants (IESBA Code), at a European and international level, we consider the European audit profession as appropriate and suitable practitioners to perform assurance engagements for the EUCS Cloud Services Scheme.

The IESBA Code requires auditors to comply with principles of professional ethics for their public interest roles, including the principles of independence, integrity, objectivity, professional competence, due care and professional scepticism. Pursuant to ISQC 1 (International Standard on Quality Control), auditors are required to establish quality control policies and procedures at firm and engagement level relating to the internal organisation of the firm. These are designed to secure compliance with decisions and procedures at all levels of the audit firm or of the performance of engagements by the auditor. In addition, auditors and audit firms are subject to an internal and external quality assurance system, in which, for example, inspections of the quality control system and of audit engagements are conducted, and the results of those inspections are to be published annually.

Based on these requirements in relation to their regulated activities, auditors are suitable assurance practitioners for the EUCS Cloud Services Scheme.

Consequently, the profession should not be obliged to take part in an additional formal accreditation process.

Application of ISAE 3000 and ISAE 3402

Another point we would like to make is that the audit methodology of ISAE 3000 and ISAE 3402 cannot be applied in isolation. Their application must be embedded in the context of the other relevant provisions of the ISAEs, which are essential for their appropriate application. These provisions are, in particular:

- Members of the engagement team and the engagement quality reviewer (for those engagements for which one has been appointed) are subject to the IESBA Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Professional Accountants (the IESBA Code), or other professional requirements, or requirements in law or regulation, that are at least as demanding as the IESBA Code [see ISAE 3000 (Revised) paragraph 3(a) in connection with A30 to A34];
- A practitioner performing the engagement is a member of a firm that is subject to International Standard on Quality Control 1 (ISQC 1), or other professional requirements, or requirements in law or regulation, regarding the firm's system in quality control, that are at least as demanding as ISQC 1 [see ISAE 3000 (Revised) paragraph 3 (b) in connection with A61 to A64];
- The engagement partner responsible for the engagement has competence in assurance skills and techniques developed through extensive training and practical application [see ISAE 3000 (Revised) paragraph 31 (b) in connection with paragraph 12 (b) and A9], recognizing that ISAE 3000 (Revised) has been written in the context of a range of measures taken to ensure the quality of assurance engagements undertaken by professional accountants in public practice, such as those undertaken by IFAC member bodies in accordance with the IFAC's Member Body Compliance Program and Statements of Membership Obligations, including competency requirements, such as education and experience benchmarks for entry to membership, and ongoing continuing professional development as well as lifelong learning requirements [see ISAE 3000 (Revised) paragraph A60 and (a) thereof];
- The practitioner has an understanding of the entire ISAE 3000 (Revised) and ISAE 3402, including their application and other explanatory material, to understand the standards' objectives and apply their requirements properly [see ISAE 3000 (Revised) paragraph 16 in connection with A23 to A28];
- The practitioner complies with relevant requirements in ISAE 3000 (Revised) and ISAE 3402 [see ISAE 3000 (Revised) paragraph 17 in connection with paragraphs 18 and A29].

We strongly recommend emphasizing in the EUCS scheme that the application of ISAE 3000 or ISAE 3402 requires the fulfilment of additional requirements as noted in the bullet list above. We note that the audit profession in the EU, and in particular in Germany, fulfil these requirements.

Assurance levels

In addition, we believe that the assurance levels “substantial” and “high” are the most relevant assurance levels. These assurance levels represent a reasonable level of assurance equivalent to, for example, the German Federal Office for Information Security [“Bundesamt für Sicherheit in der Informationstechnik (BSI)”] required assurance level “substantial” for the Cloud Computing Compliance Criteria Catalogue (C5) engagement. We are concerned that the qualitative difference between the assurance level “basic” and “substantial” is not sufficiently clear from a CSP perspective.

We suggest including more details about the differences between the assurance levels “basic” and “substantial” from a CSP perspective.

Guidance material

Finally, we would like to emphasize that, based on our experiences during the development of ISAE 3000 and ISA 3402 at the IAASB and the transposition of these standards for the German profession (e.g. IDW PS 951nF, IDW PH 9.860.3 etc.), it is vital for the application of these standards that guidance be provided with respect to the assurance report, as well as for management’s description of internal control, including management’s assertion on the design, implementation and effectiveness of those controls, of the cloud service provider (CSP).

We suggest providing guidance with respect to the issuance of the assurance report and management’s description of internal control.

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

Melanie Sack
Chief Operating Officer

Andreas Pöhlmann
Technical Director Digitalization