INSTITUT DER WIRTSCHAFTSPRÜFER

April 30, 2021

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

Accountancy Europe
Harun Saki
Avenue d'Auderghem 22-28
1040 Bruxelles
Belgien

submitted via email to: harun@accountancyeurope.eu

**Re.: Accountancy Europe's Views & Ideas Paper entitled "Fraud: Recommendations to strengthen the financial ecosystem"**

Dear Harun

The IDW is pleased to have the opportunity to comment on Accountancy Europe's Views & Ideas Paper entitled "Fraud: Recommendations to strengthen the financial ecosystem".

We fully agree that recent cases of fraud as well as the potential impact of the ongoing COVID-19 pandemic may have in terms of its potential to foster fraud indicate a need to reconsider the way in which the entire financial reporting ecosystem currently functions, including the role of auditors. Indeed, whilst the first line of defense against fraud has to be within an entity itself, each aspect of the ecosystem, including standard setters, auditors, financial supervisory authorities and prosecutors demands careful consideration, as do the interactions between the individual players within this system.

In the wake of the Wirecard case, the IDW published an IDW position paper: "Further development of corporate governance and controls as first lessons from the Wirecard case": https://www.idw.de/blob/124612/cfbb7df12ed31cd1be579bda4aa78431/down-positionspapier-wirecard-englisch-data.pdf to which we refer in discussing ACE's paper and suggestions.

In the context of fraud, the IDW suggests that management be required to establish an appropriate and effective compliance management system, designed to prevent white-collar crime in the form of fraudulent financial reporting or misappropriation of assets (anti-fraud management system) aligned to the entity's specific risk situation. Management would then report publicly on the basic features of the system and issue a statement confirming that it has established and is operating such a system appropriately. As part of its supervisory responsibilities, the Supervisory Board (this could also be tasked to the Audit Committee) would be responsible for monitoring management's compliance and then also examine whether management has fulfilled its duty to establish a workable, appropriate and effective compliance management system, publishing a statement on the results of its examination. The auditor could provide enhanced support to the Supervisory Board in performing its monitoring function, by performing audit procedures on the appropriateness and effectiveness of the compliance management system to be set up by management as part of the audit of financial statements.

The IDW's paper also made a number of recommendations as to the role of various supervisory and enforcement authorities and the need for improved transparency and effective coordination and cooperation between them.

One relevant issue not addressed in ACE's paper but discussed by the IDW is the role of further capital market participants. The Wirecard case raises questions about the lack of market reaction to information concerning publicly known deficiencies in Wirecard's corporate governance and the fact that financial reporting needs to be better adapted to the challenges of the modern digital world. Today's corporate reporting provides insufficient information about the characteristics of relevant value drivers in an entity. Changes in these areas ought also to be considered in a holistic approach to fraud.

We would like to make a few general comments before commenting specifically on the Paper's recommendations and ideas.

***General comments***

**Expectations must be realistic as to the role of the audit in prevention and detection of fraud, including highly sophisticated fraud and the cost to society of strengthening the auditor's ability to detect fraud must be weighed carefully**

We agree that it is important for the Paper to explain that there remains an unavoidable risk that some material misstatements of the financial statements may not be detected by an audit performed in compliance with the ISAs.

Whilst there is a valid expectation that an auditor will consider fraud (ISA 240.11) throughout the audit, there is often an unrealistic public expectation that the involvement of an independent auditor should always serve to detect or prevent fraud. In this context we refer to ISA 240.06-08. Furthermore, it appears that many outside the auditing profession do not fully understand the current risk-based audit model, including the auditor's application of the concept of materiality and the resulting limitation to the ability of an auditor to detect fraud.

The relationship between the cost of an audit and the degree to which an audit could reasonably be expected to detect fraud is an issue that demands careful consideration. Whilst an increase (or change) in the auditor's work could potentially improve fraud detection and prevention, any such improvement may be disproportionate in terms of the increased cost of audit. In this context, we refer to the IDW's letter to Tom Seidenstein dated February 1, 2021, https://www.idw.de/blob/128518/06dcd7873261cf58159ea893cd54e891/down-iaasb-fraud-goingconcern-data.pdf in which we noted the need to reflect on costs in a consideration about adding robust or enhanced procedures to the current audit model. We also outlined in that letter that we believe it unlikely that a "silver bullet" will become evident that has hitherto eluded standard setters.

**Recommendations should not be limited to public interest entities (PIEs)**

Whilst we generally support Accountancy Europe's initiative, we are concerned that the recommendations discussed in the Paper are limited primarily to those entities defined in EU legislation as public interest entities (PIEs) and this segment of the audit market. We believe this focus is misplaced, as fraud is not confined to PIEs. The SME sector is highly systemically relevant in most jurisdictions. Indeed, the motivations underlying fraud and the ways in which fraud might be perpetrated likely differ considerably between most owner-managed businesses and PIEs. We would therefore welcome a fuller consideration of suggestions appropriate to non-PIEs.

Indeed, it is especially important to note that the primary responsibility of management and those charged with governance for the prevention and detection of fraud as noted on page 5 of the Paper holds true for all entities, irrespective of their size, complexity or level of public interest.

As we explain below, we do not believe that it would be appropriate for all audits to be required to employ forensic experts. Furthermore, expectations as to the application of forensic methodology need to be realistic, since the application of forensic methodology can never guarantee that fraud will always be detected during the audit.

In general, there is an urgent need for our profession to take a proactive stance and be clear about the audit and its capabilities and limitations in regard to fraud. On the one hand – the ISAs specifically require auditors to address fraud and there is an entire standard ISA 240 devoted to this – thus there are public expectations that auditors will uncover fraud. On the other hand, an audit is subject to various inherent limitations which mean that highly sophisticated fraud featuring deliberate deception coupled with extensive collusion with external parties and widespread falsification of records etc. may not be detected, especially since auditors do not have powers akin to those applicable to criminal investigations. Even more challenging for non-auditors to understand is the interplay of the risk-based audit approach combined with a focus on materiality, which may result in non-material fraud slipping through the net. Since what may start out as small-time fraud may rapidly escalate to become highly significant, confusion is understandable as to why fraud may not be detected early enough. Non-auditors need to be better informed in order to understand the practical implications of these aspects. Currently, some of the public's expectations as to the auditor's role in relation to fraud detection may simply not be reasonable.

***Comments on the recommendations***

**Require companies to have and publicly report on a fraud risk management system**

This disclosure could be made as part of a broader statement included in a company's management report, along with statements on the internal controls over financial reporting. However, care would need to be taken that such a statement remain entity specific, useful to users and not use boilerplate language.

**Pay specific attention to senior management fraud: strengthen the functioning of audit committees and mandate an audit committee in all public interest entities**

We firmly agree that a well-functioning supervisory body including an Audit Committee comprising well-qualified individuals is needed as a key line of defense within a company to prevent and detect fraud – especially management fraud. We agree that an Audit Committee should be a mandatory requirement for all PIEs.

It is important to ensure that key individuals serving within an Audit Committee possess appropriate experience in financial reporting and auditing, so as to be well positioned to challenge – and where necessary stand up to – management and communicate effectively with the auditor.

In addition, Audit Committees should be required to consider audit quality and in so doing also ensure that auditor remuneration is appropriate and not artificially low as a result of hard bargaining with management or procurement departments. Overly competitive audit fees should not be accepted at the expense of audit quality.

**Make early warning mechanisms for auditors effective**

We agree that improved coordination and clarification of the responsibilities of all parties in the ecosystem is needed. However, the total extent of any failures as well as potential improvements in prevention and detection of sophisticated management fraud are still being explored in Germany. Confidentiality requirements must not serve to prevent the auditor and authorities receiving fully the information needed to fulfill their respective roles appropriately.

**Clarify auditing standards for a common understanding of the auditor's role**

ISA 240 already clarifies the auditor's role in relation to fraud. However, it is apparent that the audit model and its relation to non-material fraud is not well understood outside the auditing profession, as we have explained above.

We believe that standard setters such as the IAASB should consider – as the Paper suggests – how better to publicly communicate what an audit entails and what it does not entail, including the very significant differences between a forensic audit and the audit of financial statements in compliance with ISAs together with the reasons underlying the inherent limitations of an audit as noted in the ISAs.

The IDW also suggests it would be helpful for the ISAs to address more clearly the auditor's role regarding fraud detection when the auditor has reasonable grounds to suspect possible fraud that may lead to a material misstatement of the financial statements, linking such suspicions (risks) to specific audit procedures (risk responses). Currently various paragraphs in ISA 240 require further investigation in specific circumstances without specifying this appropriately. In our letter to the IAASB referred to above, we suggest that it may be worth exploring three issues in particular:

1. Whether the connection between fraud risk factors and the assessment of (*material*) misstatement risk at the financial and assertion levels is adequate,

2. Whether more clarity could be given as to when indications for material misstatements due to fraud in the financial statements are strong enough for auditors to need to take further measures, and
3. When auditors may need to be required to undertake forensic measures due to the risk of material misstatement in the financial statement due to fraud.

**Improve auditors' access to knowledge and awareness about fraud**

We support measures to promote a keen awareness of fraud potential amongst auditors. Training and continuing professional education – also within audit firms – should generally foster an appropriate awareness.

However, sharing information as to the nature of frauds previously uncovered cannot comprehensively arm auditors who encounter highly sophisticated and new fraud methodologies, nor can it address the way in which hitherto undetected minor frauds may often spiral to have a material impact on the financial statements in a relatively short space of time. In general, auditors will remain largely unable to detect all material frauds.

**Auditors to clearly communicate their work and conclusions about fraud**

In our view, there are three key aspects associated with auditor communication regarding audit procedures addressing potential fraud.

Firstly, effective two-way communication between the auditor and management and, possibly more importantly and more extensively (i.e., including the planned audit approach), between the auditor and those charged with governance about both potential and suspected fraud-related issues would be helpful. ISA 240.18-.20 and ISA 240.21-.22 respectively cover this, but are written in an auditor-driven way, since auditing standards cannot govern the actions of others including management and those charged with governance. It is therefore essential that both management and those charged with governance accept and comply with their responsibilities and ensure effective communication with the auditor concerning fraud. In the IDW's Position Paper mentioned above, we also highlighted the need for the Audit Committee to communicate regularly with the auditor, without the presence of management, whereby this exclusion should be set forth in the Audit Committee's procedural rules. We believe that this would allow a frank and honest exchange of views between the auditor and those charged with governance (here, the Audit Committee).

Secondly, when an auditor identifies or suspects fraud has occurred, ISA 240.41 et seq. requires – within the limits of the prevailing laws and regulations – communication with management, with those charged with governance and to an appropriate authority outside the entity. However, unless identified or suspected fraud results in a material misstatement of the financial statements, ISA 240 does not require such reporting in the publicly available auditor's report, for a variety of reasons.

We are concerned that in proposing routine reporting of an auditor's conclusions on fraud in the publicly available auditor's report – even when there are no suspicions – ACE's suggestion might lead to an expectations gap, as this would most likely generate expectations that the entity whose financial statement have been audited is entirely free of all fraud whatsoever. Amongst other things, publicly reporting on suspicions that may subsequently prove to have been unfounded would also open the auditor to be charged with having make false and libelous accusations.

We support the possibility for an auditor to obtain assurance and report on management's statement on its fraud risk management system (provided there is a suitable framework governing such a system with which management is required to adhere and report on). For certain entities such as PIEs, it might be appropriate to require this as part of the statutory audit, although voluntary assurance engagements would be helpful in many entities in certain situations. We are not convinced that this would always imply the auditor must obtain assurance of the entire internal control system over financial reporting.

Thirdly, as explained in ISA 240.05-.07, the inherent limitations of an audit mean that both instances of fraud that result in material misstatement of the financial statements and minor fraud may not be detected. Furthermore, any instances of fraud identified or suspected that do not result in material misstatement of the financial statements will not be reported publicly but are instead reported to those charged with governance such that appropriate measures can be taken to address them.

It is also important that the public understands that the financial statement audit is neither intended nor designed to fulfill the same role of a forensic audit. Improved communication by parties other than the auditor via the auditor's report is needed in this regard.

### *Specific comments on the ideas*

#### Considering more extensive use of forensic experts by auditors

In our view, using forensic methods may be an appropriate risk response if the auditor has reasonable grounds to believe that a fraud may have been perpetrated that has a greater than acceptably low level of risk of resulting in a material misstatement of the financial statements, or is engaged to specifically perform such testing in addition to the “normal” audit. As the Paper points out, this is common practice already to varying degrees, and many audit procedures have forensic elements that may not demand forensic experts.

However, we do not believe that it would be appropriate for all audits to be required to employ forensic experts. Indeed, this is simply not practicable and would not only be extremely costly, but it would also make audits irrelevant in terms of timing.

In the IDW’s Position Paper: “Further development of corporate governance and controls as first lessons from the Wirecard case” referred to above, the IDW notes its intention to develop an auditing practice note to highlight the importance of the analysis of the risk situation in relation to fraud, during audit planning. In particular, this will outline which risk responses should include forensic audit procedures - applying modern technologies.

The IDW also explained that it shares the opinion expressed by Prof. Dr. Thomas, CFO of Siemens AG ("We have to fight for the reputation of the financial centre", Börsenzeitung, 04.07.2020, p. 8) that consideration should also be given at entity level to establishing such forensic elements as part of the internal monitoring system. The IDW suggests that this would make sense, especially when dealing with information provided by whistleblowers.

**Considering more extensive use of data and technology by auditors**

The Covid-19 pandemic has arguably accelerated auditors’ use of data and technology. We also note the concerns that ACE expresses and agree that while more use of data and technology may increase the ability of auditors to detect material fraud, technology also provides fraudsters with increased means of perpetrating fraud. There will always be an “arms race” between cybersecurity and cybercrime.

Please let us know, should you have any questions, as we would be pleased to discuss this with you further.

Yours truly,

Melanie Sack
Executive Director

Gillian Waldbauer
Head of International Affairs

541/584