KPMG LLP
Audit
15 Canada Square
London E14 5GL
United Kingdom

Tel +44 (0) 20 7311 1000
Fax +44 (0) 20 7311 3311

Private & confidential
Kate Dalby
Financial Reporting Council
125 London Wall
Moorgate
London
EC27 5AS

Your ref Exposure Draft ISA (UK) 250

Our ref ISA (UK) 250/2X0

12 January 2024

Dear Kate

Proposed ISA (UK) 250 (Revised) and ISA (UK) 2X0 (Revised) Invitation to Comment and Impact Assessment

I am writing on behalf of KPMG LLP in response to the Financial Reporting Council ("FRC")'s Invitation To Comment on International Standard on Auditing ("ISA") (UK) 250A *Consideration of Laws and Regulations in an Audit of Financial Statements*, ISA (UK) 2X0 *Special Considerations for Public Interest Entities – Communicating and Reporting to an Appropriate Authority Outside the Entity* and the accompanying Exposure Drafts ("the EDs").

As set out in the FRC Remit Letter[1] from the Secretary of State for Business and Trade, and the FRC's response[2], the FRC plays a crucial role in ensuring the UK upholds high standards of corporate governance, reporting and audit. In line with the FRC's statutory growth duty, requirements and expectations must be proportionate and support growth in the UK economy. As currently drafted, we are concerned that the potential unintended consequences of the EDs appear inconsistent with the FRC's growth duty, because the burden placed on auditors and entities would be significantly larger than envisaged by the FRC's impact assessment.

In particular, the removal of the distinction between the auditor's responsibilities over laws and regulations generally recognised to have a direct effect on the financial statements ("direct" laws and regulations) and other laws and regulations for which non-compliance may have a material effect on the financial statements (which we term "indirect" laws and regulations in our response), combined with the requirement to assess risks of material misstatement related to laws and regulations to which the entity is subject, will require the

[1] Letter from Secretary of State Kemi Badenoch to Richard Moriarty, CEO Financial Reporting Council, 22 November 2023 (publishing.service.gov.uk)
[2] https://assets.publishing.service.gov.uk/media/655deff3d03a8d001207fe73/letter-from-richard-moriarty-ceo-financial-reporting-council-to-secretary-of-state-kemi-badenoch-22-november-2023.pdf

consideration of a significant number of laws and regulations – particularly for multinational groups. The proposed auditor's objectives would involve extensive additional work by both audited entities and auditors, and we envisage would often require the involvement of auditor's experts in identifying and assessing relevant laws and regulations, even in areas where the auditor ultimately determines that there is no risk of material misstatement of the financial statements.

Additionally, in our view, the proposals for ISA (UK) 2X0 go beyond what the Kingman review originally proposed, and also move ahead of the primary legislation which the Government had concluded was a necessary precursor for implementing the "Duty to Report" recommendations.

Appendix 1 to this letter provides our response to each of the questions in the *'Invitation To Comment'*, along with our further analysis. Please contact me if you have any questions on this response.

Yours sincerely

Ian Freeman
Partner, Head of DPP Audit

Appendix 1: Response to invitation to comment and impact assessment

Proposed ISA (UK) 250 (Revised) *Consideration of Laws and Regulations in an Audit of Financial Statements*

Overview

Revisions to the auditor's responsibilities – cost implications for auditors and audited entities

We agree with the aim of clarifying auditor's responsibilities in relation to laws and regulations. However, our key concern is that in doing so, the ED significantly expands the audit work required under the standard. At the heart of this concern is the removal of the distinction between the auditor's responsibilities in relation to direct and indirect laws and regulations. We believe that there is an important distinction between the two; currently the auditor performs a greater depth of testing on areas which directly affect the financial statements and performs specified procedures in respect of those laws and regulations which only affect the financial statements when they are breached.

The ED removes this distinction, and requires the auditor to identify all laws and regulations with which non-compliance may have a material effect on the financial statements (ED ISA (UK) 250.11-1(a)). Particularly for large, complex or multinational entities, it may be unachievable to identify all such legislation, given the range of areas that would need to be considered (necessitating the expertise of lawyers specialised in each of these areas of the law) and the ways in which non-compliance could affect the financial statements – through regulatory sanctions, litigation in the civil courts or through other routes.

As a result of increased questions from auditors, the ED is likely to increase the audited entity's own costs in providing the information required for the audit, in addition to the increased audit fees necessitated by the auditor's expanded work. For example, auditors would request the directors to compile a list of all the relevant areas of laws or regulations as a starting point for their work, while the auditor in turn would commonly need to involve an auditor's expert to help assess the entity's list, potentially in each jurisdiction in which the entity operates.

We also noted that the standard as drafted increases the requirement on the auditor beyond that of the directors of the company – for example, requiring the auditor to assess the risk associated with a breach in health and safety laws and regulations in an overseas subsidiary, when the directors in the UK would not be required to do this for a subsidiary outside the UK.

Difficulties in identifying and assessing risks of material misstatement

The auditor's next objective (ED ISA (UK) 250.11-1(b)) is to identify and assess risks of material misstatement ("RMM") of the financial statements arising from both error and fraud relating to non-compliance with laws and regulations. In considering a specific law or regulation, an RMM is the product of the risk that the penalty for (or other consequence of) non-compliance is material to the financial statements, combined with the risk that the entity has not complied with the law or regulation.

It is difficult, even with expert legal support, to assess the potential level of penalties and other consequences with certainty. For example, there may be a lack of historical published penalties, no published scale of fines, a lack of clear history of the level of settlements reached in the civil courts, or where the potential may exist for record fines which exceed those levied in the past to be imposed. Similarly, assessing the risk that the entity has not complied with a particular piece of legislation, if there is not a known instance of non-compliance, is still more difficult and judgemental to assess. In our view, it is insufficiently clear from the ED how the auditor would develop an appropriate basis for such an assessment, as required to comply with ISA (UK) 315.13.

While the ED provides additional risk assessment procedures, it does not address how the auditor uses what they have learned to identify and assess risks of material misstatement from amongst the relevant areas of law or regulation, since the requirements of paragraph 14-1 cross-refer to non-existent paragraphs of application guidance.

Obtaining sufficient appropriate audit evidence

Where the auditor concludes that there is scope for a breach of a certain law or regulation to result in material penalties or other consequences, and that there is a low but not remote probability of such a breach having occurred, the auditor identifies an RMM. However, it is unclear how the auditor should respond in such a circumstance; while the extant standards are clear in respect of how the auditor responds to a known breach (e.g. where the entity is the subject of litigation or claims, the requirements of ISA 501 apply, and where there is a RMM related to possible provisions or contingent liabilities, the auditor applies ISA 540 in respect of these estimates), it is not clear to us how the auditor could obtain sufficient appropriate audit evidence with respect to an area of law or regulation for which no breaches are known to the entity, given the inherent limitations of the audit in this area, as noted in the application guidance (paragraph A8-1).

The auditor's audit procedures and conclusions as to which RMMs exist over non-compliance with laws and regulations, and as to whether sufficient appropriate audit evidence has been obtained in respect of such RMMs, draw substantially on information that is known to management (and/or those charged with governance) and has been disclosed to the auditor.

In our view, it would be difficult for an auditor to detect breaches of law or regulation that are unknown to the entity, even with very extensive, appropriately designed procedures. To help demonstrate why this is, we provide a worked example of how the auditor may perform appropriate procedures but still not detect a breach of the General Data Protection Regulation ("GDPR") in Appendix 2 of this response.

Where a breach subsequently comes to light, the press or others might suggest, with the benefit of hindsight, that the auditor should have detected the breach in the course of the audit. In the case of a properly planned and performed audit, the auditor's defence to this is that they have performed the procedures the ISAs say are necessary to identify, assess and obtain sufficient appropriate audit evidence over RMMs, so it is particularly important for any revision to the ISA to be clear about what procedures the auditor does and does not need to perform to achieve this.

While paragraph A8-1 acknowledges inherent limitations even in a properly planned and performed audit that may make breaches difficult to detect, in our view, the ED as currently drafted is not sufficiently clear as to how these limitations affect the auditor's broadened objectives over what would currently be considered as indirect laws and regulations. We additionally noted that, while the ED prescribes extensive risk assessment procedures for the auditor to perform, it offers no new requirements or guidance on responding to risks of material misstatement, merely repeating the requirement of ISA 330 to design and perform further audit procedures (paragraph 15-1). This lack of clarity is another reason why we are concerned about the proposed changes to the auditor's responsibilities.

In our view, the existing standard is more proportionate, in that it focuses the auditor's response to indirect laws and regulations on addressing the consequences of identified or suspected breaches. This allows appropriate procedures to be more readily designed, and facilitates better focus on the financial statements rather than on areas of operational laws or regulations which may be far removed from financial reporting matters.

Implications for group audits

The ED does not provide specific guidance on how to apply its requirements to group audits. Given, as we have noted earlier in this response, the implications of the ED may be more extensive for group audits, particularly those operating in multiple jurisdictions, we feel this is an important area to explore and further define.

A further concern is that the ED's proposals may present execution challenges for auditors because the UK's ISA for laws and regulations would represent one of the areas of most significant divergence from the international standards that component auditors would be familiar with and trained in.

Conclusion on ED ISA 250

Overall, we recommend preserving the distinction and differentiation of work effort between the auditor's responsibilities over direct and indirect laws and regulations.

Q1. Do you agree that the proposals in ISA (UK) 250 appropriately address the public Interest?

It is not immediately clear to us what aspect of the public interest the FRC is seeking to address by revising this ISA. Since the standard will significantly increase the time spent by audited entity management, and by audit firms in auditing this area, it is likely that the cost of the audit will increase, in some cases, very considerably, and that audited entities may also incur considerable legal costs. The increased focus in this area may also poses a distraction risk from other areas of the audit, and may not be in the public interest. We are concerned that, in this instance, any benefits are outweighed by the increased burden and cost on entities, particularly given that the ED, while strengthening the auditor's responsibilities in some respects, itself lacks clarity in a number of important respects.

Q2. Do the proposed requirements in paragraphs 12-2 and 12-3 support auditors to be able to identify those laws and regulations with which non-compliance may have a material effect on the financial statements?

As explained in the overview above, we have concerns about the proposed changes to the overall responsibilities amended in paragraph 11-1[3] and reflected in the additional requirement 12-1.

Paragraph 12-2 responds to the auditor's revised responsibilities by rewording the risk assessment procedures that are already required by paragraph 13 of the extant standard, though (excluding the effect of the change in scope occasioned by the auditor's revised objectives, our concerns on which we have already laid out at some length) the altered wording does not appear materially to change the procedures required.

We agree that paragraph 12-3 provides a useful prompt to seek the entity's views on whether there are deficiencies in internal control over the prevention and detection of non-compliance (paragraph 12-3(a)(ii)b).

[3] The auditor's responsibilities currently differ depending on whether a law or regulation is direct or indirect in its effect on the financial statements, with the auditor required in the former case to "obtain sufficient appropriate audit evidence regarding compliance with the provisions of those laws and regulations", while for indirect laws and regulations "the auditor's responsibility is limited to undertaking specified audit procedures to help identify non-compliance with those laws and regulations that may have a material effect on the financial statements".

Given that the auditor's procedures include, but need not necessarily be limited to, those listed in paragraph 12-3, it would be helpful to provide further examples of procedures the auditor could additionally perform in application guidance.

We are therefore of the view that paragraphs 12-2 and 12-3, in conjunction with the auditor's revised objectives in paragraph 11-1 of the ED, would increase the extent of the auditor's work in pursuit of the revised objectives, but without a clear benefit proportionate to the significant increase in work effort.

Q3. Do you believe that the proposals in ISA (UK) 250, considered collectively, will enhance and strengthen the auditor's identification of risks of material misstatement of the financial statements due to fraud or error relating to non-compliance with laws and regulations?

As with Q2, this question is predicated on a change to the auditor's objectives which we do not agree with. As our overview explained, our areas of particular concern include the difficulties in assessing RMMs across the broad spectrum of laws and regulations which could be relevant. In particular, we note the following:

- The ED would be complex to apply to the largest entities – in particular, multinationals – and, while the additional work effort would be lower for a simpler organisation, it could still prove to be a disproportionate burden for smaller owner-managed businesses with more limited management capacity. However, even in the case of a reasonably simple business, the requirement would still be onerous in terms of establishing the panoply of laws and regulations that may apply and assessing their potential materiality.
- Even with a complete list of laws and regulations, it may be extremely challenging for the auditor to identify a breach in law or regulation which the entity itself is unaware of (see the worked example on GDPR in Appendix 2).
- The ED itself acknowledges (in paragraphs 9-2 and A8-1) that there are inherent limitations in the auditor's ability to detect material misstatements of the financial statements related to non-compliance with laws and regulations – particularly so the further removed the non-compliance is from the financial statements. However, in our view, it is insufficiently clear how these limitations affect the auditor's broadened objectives over indirect laws and regulations – in other words, how these acknowledgements act as a defence for the auditor who has planned and performed appropriate procedures but not detected a breach of law or regulation in the period in which it occurred.
- Paragraph A15-2 directs the auditor to consider the requirements of ISA (UK) 240 where the non-compliance is intentional. However, as with paragraph A18-1 of the extant standard, it is unclear which aspects of ISA (UK) 240 that the auditor should consider. Moreover, breaches of law or regulation may not necessarily fit cleanly into the two types of intentional misstatements that ISA (UK) 240 requires the auditor to

assess (misstatements resulting from fraudulent financial reporting, and misstatements resulting from misappropriation of assets). For example, suppose the entity has knowingly failed to pay the minimum wage to their employees, and therefore breached minimum wage legislation. In this instance, where the entity has correctly accounted for the (insufficient) salary cost paid, do the FRC believe that this would meet the requirement for fraudulent financial reporting and therefore require ISA (UK) 240 to apply? Any revision to ISA (UK) 250A represents the opportunity to clarify the questions which emerge from the addition of paragraph A18-1 when the ISA was revised in 2019.

Q4. Have appropriate enhancements been made to the application material?

Other parts of our response make observations on the potential for enhancements to aspects of the application material.

We also noted that certain introductory and requirement paragraphs make reference to non-existent paragraphs of application guidance. For example, paragraph 5-1(b) refers to application guidance paragraph A13, but no such paragraph exists.

Q5. Do you support the deletion of the Appendix on "Money laundering, terrorist financing and proceeds of crime legislation in the United Kingdom"?

No. In our experience, Appendix 1 in the existing standard provides useful guidance in summarising the relevant legislation and how this applies to auditors. Without it, practitioners would need independently to ascertain this information which may lead to different awareness and interpretations of the legislative requirements. We recommend retaining this guidance in any revised standard.

Q6. Do you agree with the proposed effective date for audits of financial statements for periods commencing on or after 15 December 2024?

Before issuing a final standard, we recommend that the FRC take time to reconsider whether the changes in the ED are proportionate and achieve the objectives of revising the standard. We would welcome a revised exposure draft to explore how the ISA might be most effectively updated to use the best features of the ED, whilst avoiding the challenges inherent in expanding the auditor's responsibilities in the way the current draft does. To allow time for this process, we would recommend postponing the effective date for a further 12 months, to make the standard effective for periods commencing on or after 15 December 2025.

Even if the FRC were to progress to finalise the standard using feedback from the current consultation, we would still recommend allowing the same additional time, given the extent of

revisions proposed in the ED which both auditors and audited entities will need time to prepare for.

Auditors will need to determine a revised audit approach to laws and regulations. Similarly, audited entities will need time to prepare additional information for audit purposes, such as a complete list of all laws and regulations to which the entity is subject, as well as an assessment of how these affect the entity which may need to draw on regulatory, legal and industry expertise. This is likely to take significant time both for large or complex groups, and for smaller entities with more limited management capacity and in-house expertise to deal with such enhanced regulatory demands.

Proposed ISA (UK) 2X0 (Revised) ***Special Considerations for Audits of Public Interest Entities – Communicating and Reporting to an Appropriate Authority Outside the Entity***

Overview

We agree with the objective of strengthening ISA (UK) 250 Section B, and we support the renumbering and renaming of the standard to separate it from (what is currently) ISA (UK) 250 Section A. However, in our view, the proposed changes as drafted do not have the proper framework to support them and, in several respects, are moving ahead of primary legislation necessary to support their effective implementation. In particular, we note the following:

- **Changes ahead of primary legislation:** Following the King's Speech in November 2023, it now appears likely that primary legislation to introduce the Audit, Reporting and Governance Authority ("ARGA"), with statutory powers to hold directors of PIEs accountable for their audit and corporate reporting duties, as well as the legislation which would ensure there are appropriate protections in place for auditors from breach of duty claims in relation to disclosures to the regulator, will not be introduced in the near term. This creates two key concerns.

  Firstly, extending the auditor's role to report public interest matters, without increasing the directors' responsibility to report these matters (who have the primary responsibility), increases the asymmetry between management and the auditor.

  Secondly, the Government concluded that statutory protections should be in place prior to increasing the auditor's duty to report. However the FRC appear to be moving ahead without this primary legislation in place. The risks for auditors increase significantly with the new proposals, particularly where the application guidance suggests that with the benefit of hindsight, auditors could be held accountable for not reporting a non-compliance matter which later leads to a financial loss (paragraph A59). Without limitation of liability and necessary statutory protections, the risk placed on the auditors could lead

to audit firms choosing to exit, or not to enter, the PIE audit market and increase the likelihood of orphaned audits.

- **Extending reportable matters to those "in the public interest":** The Invitation To Comment explains that this extended requirement was introduced following Sir John Kingman's recommendation that a duty of alert for auditors to report viability or other serious concerns should be introduced. We do not consider extending the requirement to public interest matters to be a proportionate extension of auditors' duties, and without a clear framework of what is "in the public interest", risks inconsistent application and reporting across the industry.

- **Future scope increase:** The proposed scope of ISA 2X0 is PIEs. The consultation acknowledges that it is the FRC's intention that ISA (UK) 2X0 will apply to all entities caught by any future revision to the definition of PIE. We cannot comment on whether it would be appropriate for the proposed changes to apply to all PIEs caught by a future definition. In our view, the FRC should assess this separately if there is a revision to the definition of PIE to ensure that the standard remains proportionate.

- **Detailed framework and guidance:** If these changes were to be introduced, we believe that there needs to be a detailed framework and guidance to support auditors' consistent reporting. As stated in our response to the Kingman review and BEIS's Restoring Trust in Audit and Corporate Governance, this framework would need to include details of whom such matters should be reported to, the range of matters which should be reported and the timing of such reports.

Q7. Do you agree that the proposals in ISA (UK) 2X0 appropriately address the public interest?

We do not consider that the proposals with ISA (UK) 2X0 appropriately address the public interest.

In our view, the public interest would be best served by maintaining the present, well-established regime under which auditors are expected to comply with statutory duties to report to regulators if significant matters relevant to the regulator, such as breaches in law or regulation, come to the auditor's attention. This, combined with the already established reporting on going concern, appropriately addresses the public interest.

Further, there are already significant complexities with regard to what to report and who to report to, because each regulator has different requirements as to what they wish to receive reporting on. We believe a more holistic review and simplification of the reporting regimes across regulatory authorities would lead to more appropriate reporting to the right regulators.

Q8. Do you agree with the proposed scope of ISA (UK) 2X0 being limited to public interest entities, or do you believe that the requirements of ISA 2X0 should also apply to:

a) Listed entities
b) Charities
c) Other entities in regulated industries
d) All entities?

When responding, consider that for many audits, as reportable matters are not likely to be identified, only the requirements in paragraphs 11-13 will apply and that all auditors are subject to anti-money laundering legislation.

If the proposed changes are implemented, in our view, in order to be balanced and proportionate, the scope of the ISA (UK) 2X0 should be limited to UK PIEs, as defined by UK legislation.

While there are other regulators of certain entities to whom auditors have a statutory duty to report on defined matters (for example, entities regulated by The Pensions Regulator), we are unclear how the inclusion of such entities in the scope of ISA 2X0 would provide further protection of the public interest. Given that the duty already exists, including these entities could lead to unnecessary duplication of reporting requirements.

As noted in our response to Q7, a holistic review and simplification of reporting regimes across regulatory authorities would be beneficial.

Q9. Do you support the definition of Reportable Matters?

We do not support all parts of the proposed definition of "Reportable Matters". Our comments on each part are as follows:

i. *"Is required to report to an appropriate authority outside the entity in accordance with law, regulation or relevant ethical requirements"*

We support this part of the definition.

ii. *"Has determined reporting such information to an appropriate authority outside the entity is an appropriate action in the circumstances"*

We believe that, without a clear framework on what matters should be reported and to which "appropriate authority", we do not consider this to be a proportionate addition to the standard.

iii. "Has determined is of such significance that it is in the public interest to report even where law, regulation or relevant ethical requirements do not require it"

We do not consider extending the duty to report to undefined matters "in the public interest" to be a proportionate extension of auditors' duties. The ED is not clear as to the matters the FRC intends to capture with this requirement. Greater transparency about how the regulators have acted upon (or intend to act upon) such notifications (limited to disclosure of the action to the statutory auditor and the company) will lead to a better understanding of the information the regulators are truly concerned about and could result in more relevant reporting to support the regulator in discharging their duties. This could be achieved through a dialogue between the regulatory authority, the entity and its auditor.

We also note that many regulators only want to be notified of a specified list of matters, and only want to receive the notification once (i.e. if an entity has already self-reported a matter, the regulatory authority will not want a duplicate notification from the auditor). In this respect, we note that there would need to be consideration of other reporting regimes to avoid duplication and inconsistency (see, for example, the UK Proceeds of Crime Act).

Q10. Do you believe that the proposals in ISA (UK) 2X0, considered collectively, will enhance and strengthen the auditor's identification of matters that should be reported to an appropriate authority outside the entity?

In our view, the proposals in ISA (UK) 2X0 will not enhance and strengthen the auditor's identification of matters that should be reported to an appropriate authority outside the entity.

If the proposals are introduced as currently drafted, there should be a framework for how the public interest should be determined and considered (see response to Question 11) in order to lead to consistent reporting across the industry. The lack of a well-defined framework raises concerns about identifying matters for external reporting and the consequences of reporting based solely on public interest.

Q11. Have appropriate enhancements been made to the application material?

We do not consider the wording in paragraph A59 to be appropriate, because we do not believe that the ISA should suggest that an auditor's decision may be "called into question at a future date", or that the auditor should consider the possible consequences "if financial loss is occasioned by non-compliance with laws and regulations which the auditor suspects (or ought to suspect) has occurred but decided not to report".

This wording does not provide guidance to the auditor as to the audit work to be performed to obtain the sufficient, appropriate audit evidence, and instead may be seen by third parties as

providing a basis on which to question the auditor's approach. We can foresee that if the application guidance suggests that the auditor's work in this area may be called into question readily, it may reduce the number of audit firms willing to be auditors of public interest entities. We also foresee that this wording could lead to what receiving regulators might consider to be over-reporting, which could increase burdens on numerous regulators.

Notwithstanding our response to the previous questions, if the proposed standard ISA (UK) 2X0 were to be introduced as drafted, we believe the application guidance should include the following.

- A framework for how the public interest should be determined and considered. The FRC's *General Principles for considering the public interest in our work*[4] may be a relevant starting point, though we recognise that these principles were designed with the FRC's role in mind, not the auditor's. Without a framework, there is a risk of inconsistent application of the standard, and therefore greater "warning signals" for entities audited by a particular firm.
- The guidance should also include:
    - **To whom such matters should be reported:** It is currently unclear whether the FRC is intended to be the *de facto* regulatory authority for matters in the public interest, particularly if the scope were to be extended beyond PIEs.
    - **The range of matters which should be reported:** Greater clarity on the matters to be report would lead to more consistent and useful reporting for regulators. This may also include matters which do not have to be reported.
    - **The timing of such reports:** The current wording in paragraph A34-1 includes the phrase "as soon as practical", which we do not consider to be specific enough. More specific timeframes would provide further clarity.

Q12. Do you agree with the proposed effective date for audits of financial statements for periods commencing on or after 15 December 2024?

To the extent that ISA (UK) 2X0 is simply the current ISA (UK) 250 Section B, unaltered but separated from ISA (UK) 250A, we would support of an effective date commencing on or after 15 December 2024.

However, in our view, this effective date would be premature for any further changes to the standard, given that primary legislation to form ARGA, provide it with the necessary powers to hold directors to account for their audit and corporate reporting-related duties, and the necessary protection for auditors is a prerequisite for any broadening of the requirements on auditors to report matters in the public interest.

[4] General principles for considering the public interest in our work (frc.org.uk)

If ISA (UK) 2X0 were to be introduced as drafted, we believe the effective date should only be set once a full framework of how the public interest should be determined has been finalised, which should be subject to a separate consultation.

Appendix 2: Worked examples of GDPR breach at entity

Year 1

During the year ended 31 December 20X1, an employee inadvertently emails personal and sensitive data to an external party, leading to a breach in GDPR. The employee is unaware that the email that they sent included sensitive personal data as well as the data that they meant to include, and so has not reported it to management. Management are unaware of the issue. The entity has an established training programme for all staff annually, all staff have access to the company's policy on the use of data and data privacy on the company's intranet and the internal audit function performs spot checks on data being emailed out of the company. The entity's processes and controls have not detected the breach.

Audit response in year 1

During risk assessment, the auditor designs and performs procedures to identify laws and regulations with which non-compliance may have a "material effect on the financial statements", as required by paragraph 12-1. Through the procedures suggested in paragraph 12-3, the auditor identifies that breaches by the company with GDPR legislation may result in fines of up to 4% of global turnover for the preceding financial year or €20m, but the result of the procedures undertaken (inquiries, inspection with licensing authorities, legal confirmations and review of minutes) do not identify that a breach has occurred in the period.

Where the auditor concludes that there is scope for a breach of GDPR to result in material penalties and that there is a low, but not remote probability, of such a breach having occurred, the auditor identifies a risk of material misstatement. However, in this case, the auditor might assess that the risk of a breach occurring is remote, given the knowledge they gained through risk assessment procedures on the arrangements the entity has in place to manage the risk of a breach, as described above. Therefore, in this scenario, the auditor would not detect the breach.

Even in a situation where the auditor identifies that a risk of material misstatement exists in respect of GDPR, and therefore performs additional procedures to respond to the assessed risk, such as reviewing whistle-blowing reports, confirming that all staff have received GDPR training in the year, establishing the entity has a system to monitor non-completion of training, and reviewing the work of internal audit, the auditor is still highly unlikely to detect that a breach of GDPR has occurred in this instance.

It is not evident how the auditor could obtain sufficient, appropriate audit evidence in this situation when the breach is not known to the entity.

Year 2

After the accounts for 31 December 20X1 have been signed, the entity becomes aware that the employee has sent an email which contained confidential data in the current year (20X2). In this instance, the email was copied to a colleague who identified the error and alerted management. The entity investigated the incident, and, as part of this investigation, their internal audit department scanned earlier emails from the employee that was responsible for the breach. This search highlighted the previous breach that had occurred in 20X1. The entity takes the necessary steps to raise the issue to the Information Commissioner's Office (ICO), and reports the breach to the auditor as soon as they are aware of the breach. The entity's legal advice indicates that the maximum penalty could be a fine which is material to the financial statements.

Concerns that this fact pattern raises:

- The breach is material and arose in 20X1, but even though the auditor has identified that a risk of material misstatement exists, the further procedures would not identify that this breach had occurred prior to the accounts for year 1 being signed.
- In our view, it would be exceedingly hard for an auditor to identify that a breach of this nature (that is not identified by management) exists despite executing the procedures suggested by the standard.
- The ED does not appropriately clarify whether the procedures undertaken by the auditor were sufficient in this instance. We are concerned about how a regulator or other external parties (such as the media) may interpret this.
- As articulated above, it is not evident from the ED how the auditor could obtain sufficient appropriate audit evidence in this situation when the breach is not known to the entity.