June 20, 2022

Ken Siong
Program & Senior Director
IESBA
Via Email: KenSiong@ethicsboard.org

Dear Mr. Siong:

Thank you for the opportunity to review and respond to 'Proposed Technology-related Revisions to the Code'.

About MindBridge

MindBridge is an advanced data analytics tool for auditors. Our customers include global firms as well as small medium sized practitioners (SMPs). Our technology utilizes ensemble AI to detect anomalies for auditors to better enable auditors. We are committed to transparency and explainable AI.

We have been certified as meeting ISO 27001 standards and have completed the System and Organization Controls (SOC) 2® Type 2 examination.

MindBridge is the first data audit and analysis software solution to go through The Institute of Charted Accountants in England and Wales (ICAEW) Technology Accreditation Scheme. We have been named to the Forbes AI 50, a list of private companies recognized for their contribution and continued innovation in the field of artificial intelligence. Further, we were the first private sector signatory to the Montreal Declaration for a Responsible Development of Artificial Intelligence.

Most importantly, our algorithms have received a comprehensive audit by University College London Consulting (UCLC), a renowned center of excellence for algorithm audit and safety. We were the first in their class to embark on such a code-level review of 43 of our algorithms. The UCLC audit verified that the algorithms work as designed, what the algorithms do when implemented, the review process in regard to algorithm performance, the implementation of new algorithms, and test coverage. This third-party validation provides assurance over the privacy, explainability, robustness, and unbiased nature of our algorithms and were the first to obtain such an algorithm audit

General Comments

Overall, we strongly support the project to enhance professional accountants (PA's) ability to oversight and rely on technology. Further, the overall approach to liken the ability to rely upon an output from a technology as similar to the reliance of an expert is an elegant approach to oversight. In addition, it reinforces that while technology may automate certain tasks, software tools, like ours, should be developed to support human judgement and not replace it. More importantly, as your

have learned from our background, the concept of transparency and explainable artificial intelligence (xAI) is at the ethos of our Company and tool.

Further, we understand the challenges that small and medium practitioners (SMPs) might have with some of these assessments and the resources available to them, therefore we have focused our product design and company on being forward with our explainability to further help in this regard.

Specific Responses

Technology-related Considerations When Applying the Conceptual Framework

1. Do you support the proposals which set out the thought process to be undertaken when considering whether the use of technology by a PA might create a threat to compliance with the fundamental principles in proposed paragraphs 200.6 A2 and 300.6 A2? Are there other considerations that should be included?

> We generally support the lists provided and agree with the change during the drafting process to focus on the output of technology. However, the structure of the bullet points, as written, is slightly confusing.
>
> The first three bullet points are written more as safeguards. The final bullet point is written more as a new threat/refinement of the definition of the general compliance threat.
>
> However, the second to last bullet point is unclear if this is a safeguard or a threat. Specifically, the second to last bullet point states:
>
> > "Whether the technology incorporates the expertise or the judgements of the accounting or employing organization".
>
> For example, in the case where a configuration is set based on judgement that better improves the quality of the output as fit for purpose, we see this as a supporting the PA's ability to rely upon the output. However, to the extent that judgement is implying that the technology is replacing the PA's judgement and taking over the human experience and in effect as subordinating judgement to the output, clearly that is at threat to the overall general requirements.
>
> We believe the uncertainty of threat/safeguard status of this bullet may assist in keeping the standard future-proofed as technology advances, as this is clearly the grey zone that requires PA's judgement. However, we are concerned that some may perceive this item as a threat due to the proximity to the final bullet point. Additional application guidance maybe needed to make clear that incorporating judgement to improve product output is not the same as an overall subordination of judgement.

Further, the inclusion of 220.7 A3 is exceptionally important for PAIB's as related to 200.6 A2. However, we do expect that it will be complex for a PAIB to document and ever provide historical information on if they had made such assessments if they are no longer employed by their employer. The complexity of most organization's confidentiality information and non-disclosure agreements may conflict with a PAIB's ability to show they were in compliance with the code. Paragraph 220.7 A3 may need to be expanded to further safeguard PAIB's who might be the sole PA in an organization.

Determining Whether the Reliance on, or Use of, the Output of Technology is Reasonable or Appropriate for the Intended Purpose

2. Do you support the proposed revisions, including the proposed factors to be considered, in relation to determining whether to rely on, or use, the output of technology in proposed paragraphs R220.7, 220.7 A2, R320.10 and 320.10 A2? Are there other factors that should be considered?

As written, the second to last bullet point could create undue complexity in tools provided by third parties:

> "The employing organization's oversight of the design, development, implementation, operation, maintenance, monitoring or updating of the technology."

We have already received questions on whether this means that our customers need to review our source code. As noted in the background section, we have already taken steps to provide third-party review of our code related to data science. In addition, there would be ways to oversight these processes without review of source code. Source code is considered very proprietary in many regards and most of our customers do not have the ability to competently review code. The concerning word is likely "oversight" vs. a separate term related to vendors (as compared to internally developed software). A solution maybe to use the clause "oversight or understanding of."

In addition, the concerns related to PAIB's expressed in our response to question 1 remain relevant to this question (i.e., an organization's confidentiality of information and non-disclosure agreements may conflict with a PAIB's ability to show they were in compliance with the Code).

Consideration of "Complex Circumstances" When Applying the Conceptual Framework

3. Do you support the proposed application material relating to complex circumstances in proposed paragraphs 120.13 A1 to A3?

No, these paragraphs are confusing and appear to be concepts that are usually included in practice aides. The inclusion here makes it appear that it is an additional requirement when in fact it is providing no additional requirements, instructions, or application guidance on how to navigate the Code. This appears to be a definition of what is a complex circumstance and then does not have any impact in any other place in the code.

4. Are you aware of any other considerations, including jurisdiction-specific translation considerations (see paragraph 25 of the explanatory memorandum), that may impact the proposed revisions?

No response.

Professional Competence and Due Care

5. Do you support the proposed revisions to explain the skills that PAs need in the digital age, and to enhance transparency in proposed paragraph 113.1 A1 and the proposed revisions to paragraph R113.3, respectively?

While the additional skills outline in 113.1 A1 are likely to increase the likelihood for a PA's career success, the lack of these skills should not be considered an ethical violation. For example, there are some very competent, intelligent individuals that may be neurodiverse, such as those on the autism spectrum who may have social deficits. We propose removing this bullet as we believe it may discriminate against individuals with disabilities who otherwise possess professional competence.

6. Do you agree with the IESBA not to include additional new application material (as illustrated in paragraph 29 of the explanatory memorandum) that would make an explicit reference to standards of professional competence such as the IESs (as implemented through the competency requirements in jurisdictions) in the Code?

No response.

Confidentiality and Confidential Information

7. Do you support (a) the proposed revisions relating to the description of the fundamental principle of confidentiality in paragraphs 114.1 A1 and 114.1 A3; and (b) the proposed Glossary definition of "confidential information?"

No response.

8. Do you agree that "privacy" should not be explicitly included as a requirement to be observed by PAs in the proposed definition of "confidential information" in the Glossary because it is addressed by national laws and regulations which PAs are required to comply with under paragraphs R100.7 to 100.7 A1 of the Code (see sub-paragraph 36(c) of the explanatory memorandum)?

No response.

Independence (Parts 4A and 4B)

9. Do you support the proposed revisions to the International Independence Standards, including:
(a) The proposed revisions in paragraphs 400.16 A1, 601.5 A2 and A3 relating to "routine or mechanical" services.
(b) The additional proposed examples to clarify the technology-related arrangements that

constitute a close business relationship in paragraph 520.3 A2. See also paragraphs 40 to 42 of the explanatory memorandum.
(c) The proposed revisions to remind PAs providing, selling, reselling or licensing technology to an audit client to apply the NAS provisions in Section 600, including its subsections (see proposed paragraphs 520.7 A1 and 600.6).

> We are in a unique situation as our customers are CPA Firms. Our customers range from the Big4 to SMPs. Our tool does allow the ability for a firm to configure their methodology on our product and that could be considered a solution in the final bullet point of 520.3 A2. In those circumstance, the firm does not have access to our source code and is solely providing configurations and customizations for that firm. Those are similar services we provide to all customers that are in need of such services.
>
> We do permit firms, that would like to, to use our logo and other similar mentions in using our technology on their engagements as many firms find the use of advanced analytical tools to be a value proposition in their jurisdictions.
>
> The complexity that arises for us is that we have a financial audit as well. The additional final bullet point of 520.3 A2 could make it very difficult for us to find a reputable auditor and is likely the situation for many other organizations that create audit technology. While we are happy to go through determine appropriate safeguards for any true threats, we believe the inclusion of the point, may increase false positives of threat for providers of products that allow for configurations that enhance the value of outputs for PA's.

10. Do you support the proposed revisions to subsection 606, including:
(a) The prohibition on services in relation to hosting (directly or indirectly) of an audit client's data, and the operation of an audit client's network security, business continuity and disaster recovery function because they result in the assumption of a management responsibility (see proposed paragraph 606.3 A1 and related paragraph 606.3 A2)?
(b) The withdrawal of the presumption in extant subparagraph 606.4 A2(c) and the addition of "Implementing accounting or financial information reporting software, whether or not it was developed by the firm or a network firm" as an example of an IT systems service that might create a self-review threat in proposed paragraph 606.4 A3?
(c) The other examples of IT systems services that might create a self-review threat in proposed paragraph 606.4 A3?

> We commend IESBA on clearly delineating that obtaining data for a permissible engagement is not an assumption of management responsibility (606.3 A2). This paragraph is extremely important in a PA's ability to follow data security best practices and provides flexible engagement management.
>
> In 606.3 A1, second bullet point the "an" as the second word may be more easily read as "operates as the."
>
> We also want to emphasise the importance of term "might" include 606.4 A3 with regards to what could be a self-review threat. The area of software and IT system development is moving so quickly defining the criteria to assess if there is a threat is the preferred approach over bright lines or current practices being defined as threat.

11. Do you support the proposed changes to Part 4B of the Code?

No response.

Sincerely,

Danielle Supkis Cheek

VP, Strategy and Industry Relations
MindBridge
Danielle.Cheek@MindBridge.ai