June 20, 2022

International Ethics Standards Board for Accountants ("**IESBA**")
Via online submission: https://www.ethicsboard.org/publications/proposed-technology-related-revisions-code

Dear Sirs/Mesdames:

Re: Exposure Draft – Proposed Technology-related Revisions to the Code

Thank you for the opportunity to comment on the above-noted Exposure Draft (the "**ED**").

We applaud the IESBA's project to review the robustness of its *International Code of Ethics for Professional Accountants, Including International Independence Standards* (the "Code") in light of the current environment of rapid technological advancements and its impact on the accounting profession. The information age presents new ethical challenges and complexities for professional accountants ("PAs"). As such, it is imperative that the Code evolve to guide PAs through the changes in their work processes and scope of services precipitated by technological change.

Overall, we support the IESBA's proposed revisions to the Code and agree with the principles-based approach taken. With ongoing significant developments in technology, this approach ensures that the Code continues to remain relevant and fit for purpose. We further support the IESBA Technology Working Group's plans to develop non-authoritative technology-related guidance to assist PAs in the implementation of the revisions.

Given the dynamic world of technology, we encourage the IESBA to continue to keep abreast of changes in consideration of whether future iterations and adaptation of the Code are required. Therefore, it may be appropriate to retain a technology-related research project on the IESBA's work plan.

We provide our responses below to certain of the IESBA's specific questions related to the ED.

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 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 concur with the considerations listed in paragraphs 200.6 A2 (for PAs in business) and 300.6 A2 (for PAs in public practice). The new application material will assist PAs in identifying threats to compliance when they rely on, or use, the output of technology. We

recommend adding whether the PA has access to an appropriately qualified external and/or internal expert(s) to assist them in understanding the technology as an enhancement to the existing consideration of whether the PA has the professional competence to understand, use and explain the output from the technology.

With the rapid development of information technology solutions, it will be important for professional bodies to support their members in developing and expanding their technological competencies. This support, which may include education, professional development, guidance, and other supports, will be necessary in order for PAs to effectively assess and evaluate whether technologies upon which they rely are appropriate for their purposes and any threats that may arise are adequately addressed.

We encourage the IESBA to continue its thought leadership and other support in this area.

Independence

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).***

Routine or Mechanical Services:

The ED proposes revisions relating to "routine or mechanical services" in paragraph 400.16 A1, and when providing accounting and bookkeeping services in paragraphs 601.5 A2 and A3. Paragraph 601.5 A2 highlights that the factors to be considered in evaluating whether an automated service is "routine or mechanical" includes how the technology functions. With advancements in technologies that support accounting and bookkeeping services, such as the ongoing and expanding usage of cloud-based solutions, there is increased complexity in understanding whether an automated solution is considered "routine or mechanical".

A challenge when using third-party cloud service providers is the PAs' ability to fully understand, or access, the source code to assess the complexity of the functionality and the automated processing that may be taking place within the solution. This lack of transparency to the end user makes it difficult for PAs to assess whether the technology is, or is not, routine or mechanical. However, standard functions provided by a third-party service provider may pose little or no threat to PA independence. Therefore, additional guidance and application materials to assist PAs in performing this assessment should be considered.

Overall, we agree that PAs in public practice should hold a general understanding of the technology process, be it routine or mechanical. When technology is used in performing a professional activity for an audit client, we agree with the requirement that the firm shall not assume a management responsibility and that the firm be satisfied that the client's management makes all judgements and decisions that are the proper responsibility of management.

Close Business Relationships:

The ED clarifies the technology-related arrangements that constitute a close business relationship in paragraph 520.3 A2 to include when a firm sells or resells the client's products or services, and vice versa, and/or arrangements under with the firm develops technologies jointly with the client.

A key differentiator of technology companies is that many software companies only sell their products through resellers as they have chosen not to build a sales team as part of their business model. This type of business model should not automatically trigger the resignation of a firm as auditor of that software company due to the close business relationship independence rules.

While we understand that including examples of close business relationships may detract from the principles-based nature of the Code, in this area, providing additional application material would be helpful in better understanding the nature of close business relationships related to technology that may be of most concern to the IESBA and the interrelatedness with the guidance in paragraphs 520.6 A1 and A2 with respect to buying goods or services from an audit/review client. For example, if a firm purchases software in bulk from an audit/review client which it resells to other clients as part of its bookkeeping service line, we would not consider this to create a close business relationship. In this situation, we would rely on the application material in paragraphs 520.6 A1 and A2 and conclude that the transaction is in the normal course of business and at market terms for a bulk purchase similar to an arrangement that would be negotiated with any other client who makes a larger order. Therefore, a threat to independence would not exist.

Non-Assurance Services:

We support the revisions in paragraphs 520.7 A1 and 600.6 to remind the PA that the NAS provisions in Section 600 apply for audit clients.

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 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 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 have several concerns regarding the proposed revisions to subsection 606. We believe that the proposed changes could have a significant negative impact on the accessibility of technology-related services by small to mid-sized entities, especially those who are geographically remote.

From a Canadian perspective, we have a significant number of less sophisticated small and mid-sized public companies, private companies, public sector entities and not-for-profit organizations who, therefore, place increased reliance on their professional service providers to act as a trusted advisor in both the provision of assurance and non-assurance services. While it may be feasible for larger entities to engage a separate professional service provider for non-assurance services, we believe it could be inefficient and costly for many small and mid-sized entities to do the same. Therefore, we do not believe that the same broad approach should be taken for all audit/review clients vs. those which meet the definition of a public interest entity.

a) Paragraph 606.3 A1 of the ED provides examples of IT services that, when provided to an audit/review client, results in the assumption of management responsibilities for which safeguards would not be sufficient to address the self-review threat. These examples include:

   - Providing services in relation to hosting (directly or indirectly) of an audit client's data;
   - Operating an audit client's network security, business continuity or disaster recovery function ("IT Network and Business Continuity Services").

   We highlight our concerns with respect to these two areas separately below.

   Hosting Data:

   We suggest providing additional clarity that hosting of an audit/review client's data, <u>indirectly</u> on a platform that is managed and operated by a third party, would not result in the assumption of management responsibilities. The third party performing the

hosting service would be responsible for managing the data that is stored on their platform. Therefore, it is our belief that hosting an audit/review client's data in, for example, the cloud that is hosted by a company unrelated to the firm would not result in the assumption of management responsibilities by the firm solely because of the firm's ability to access that data. We encourage the IESBA to provide additional guidance as to examples of what would be considered "indirect" hosting of a client's data which would be prohibited.

Further, paragraph 606.3 A1 seems contradictory to, and inconsistent with, paragraph 606.3 A2 which states that the collection, receipt, and retention of data provided by an audit client to enable the provision of permissible services to that client does not result in an assumption of management responsibility. We request clarification as to whether the IESBA's intent is that such data can only be retained for a specific timeframe and, if so, that this be provided as application material within the Code.

Finally, a firm may provide IT services more broadly to a similar group of entities within an industry. Some, but not all, of these entities may be audit/review clients of the firm which, based on the proposed revisions in the ED, would restrict their ability to receive benefit from these services if their data is hosted. For example, a firm may be engaged to compile and manipulate industry/operational data from entities within the same industry to present key data metrics to allow those entities to benchmark their financial and/or operational results against their peers. In our view, if the IT service that is provided to all entities within that industry is identical then it would not be appropriate to preclude audit/review clients from being able to benefit from this type of IT service solely on the basis that the firm is hosting their data. We do not believe that this type of IT service would be considered to be an assumption of a management responsibility.

IT Network and Business Continuity Services:

The prohibition in providing IT Network and Business Continuity Services, such as network security, business continuity or disaster recovery functions, will negatively impact many small to mid-sized entities. These entities face rapid technological changes which can be challenging given their relative size and available resources. It is critical for these clients to have access to IT expertise, offered by firms that possess these IT competencies, because it provides these clients with greater choice of service providers. Specifically, in the mid-market space, clients benefit from having service providers who have an in-depth understanding of their business strategy and familiarity with their operating environment, which often results in more cost-effective solutions. Also, having a technology service provider who understands how the client's auditor/accountant will need to use the system for purposes of the audit/review provides value-add to the client.

Further, paragraph R606.3 precludes a firm from assuming a management responsibility when providing IT system services to an audit/review client without adequate safeguards. It is our view that the application of the safeguards listed in paragraph R606.3 (a) to (d), adequately mitigate potential significant independence

threats arising from either hosting client data or providing IT Network and Business Continuity Services for small and mid-sized entities. Therefore, we recommend that the prohibitions for hosting data and IT Network and Business Continuity Services should only be for those entities which meet the definition of a public interest entity or when appropriate safeguards cannot be applied.

Lastly, the proposed revisions to the Code in paragraph R606.3 appear to suggest that the provision of cyber security services would be prohibited for all audit/review clients. Under the Canadian independence rules, a firm is not prohibited from being engaged by those charged with governance of an audit/review client to assist them in fulfilling its responsibilities to conduct its own investigation of a potential accounting impropriety (e.g. fraud). We believe that an analogy could be made with respect to assisting those charged with governance of an audit/review client in assessing the financial impact of a cyber security threat and/or breach. Therefore, we do not feel that all cyber security services should be explicitly prohibited for all audit/review clients so long as appropriate safeguards are in place (e.g. separate engagement teams, an appropriate and competent member of senior management at the client makes all management decisions, etc.).

b) The presumption of implementing "off the shelf" ("**OTS**") software contained in extant paragraph 606.4 A2 should be retained. There are currently many software applications on the market, including both on-premise and cloud based solutions (e.g. QuickBooks, Simply Accounting, Microsoft Suite, etc.), that do not require any significant customization. We foresee this continuing as new technologies are developed. Therefore, the extant presumption that OTS software would not usually create a threat as long as a management responsibility is not assumed by individuals within the firm continues to be relevant and should be retained. Small to mid-sized entities are not implementing sophisticated or complex software that larger organizations are. Therefore, removal of this exception is putting such entities at a disadvantage.

   If the IESBA is concerned that this exception has historically been inappropriately applied, we recommend further application material be developed in place of the removal of the exception. For example, the Code could provide examples of the difference between "configuration" (e.g. modifying the program's code) which may be inappropriately applied vs. "customization" (e.g. creating a report based on criteria established by the client where the reporting functionality already exists in the software) which may be appropriate when not significant.

c) Paragraph 606.4 A3 of the ED provides examples of IT systems services that, when provided to an audit/review client, may create a self-review threat. These examples include:

- Designing, developing, implementing, operating, maintaining, monitoring, or updating IT systems;
- Supporting an audit/review client's IT systems, including network and software applications; and
- Implementing accounting or financial information reporting software, whether or not it was developed by the firm or a network firm.

Overall, we agree that the above-noted types of IT systems services may create a self-review threat. In accordance with paragraph R606.6 of the Code, these services are prohibited for public interest entities. Therefore, it will be imperative that Canadian standard setters appropriately refine the definition of a public interest entity to fit the Canadian landscape so that this prohibition does not negatively impair small and mid-sized entities' ability to access services with the application of appropriate safeguards.

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

Please refer to our comments above as they would also apply to the proposed changes to Part 4B of the Code. Nevertheless, we agree with the language added to confine the IT systems services prohibitions to those impacting the underlying subject matter of the assurance engagement.

MNP LLP ("**MNP**") is one of Canada's largest chartered professional accountancy and business advisory firm. Our clients include small to mid-size owner-managed businesses in agriculture, agribusiness, retail and manufacturing as well as credit unions, co-operatives, Indigenous communities and businesses, medical and legal professionals, not-for-profit organizations, municipalities and other public sector entities. In addition, our client base includes a sizable contingent of publicly-traded companies.

We appreciate the opportunity to provide feedback on this ED and look forward to reviewing the IESBA's deliberations and responses to comments received. We would be pleased to offer our assistance to the IESBA in further exploring the issues raised in our response or in finding alternative solutions.

Yours truly,

MNP LLP

Monique Côté

Monique Côté, CPA, CA
Leader, Ethics and Independence