IESBA International Ethics Standards Board for Accountants®

529 Fifth Avenue, New York, NY 10017
T + 1 (212) 286-9344 F +1 (212) 286-9570
www.ethicsboard.org

Meeting: IESBA

Meeting Location: Nashville, TN

Meeting Date: September 12-16, 2022

Agenda Item 8

Technology Project

I. Objectives

1. To consider the significant issues raised by respondents to the Exposure Draft (ED), *Proposed Technology-related Revisions to the Code*.

2. To provide directional input on the Task Force's responses to the significant issues raised by respondents to the ED and the related revisions to the proposed ED text.

> The Task Force welcomes advance comments on its responses and drafting suggestions on its revisions to the proposed ED text (i.e., **Agenda Items 8-B and 8-C**) by September 9, 2022.
>
> Please email kamleung@ethicsboard.org.

II. Background and Activities Since Last IESBA Meeting

3. On February 18, 2022 the IESBA issued proposed revisions to the *International Code of Ethics for Professional Accountants (including International Independence Standards)* (the Code) as set out in the Exposure Draft, *Proposed Technology-related Revisions to the Code* (ED) with a comment deadline of June 20, 2022. Appendix 1 of this paper includes a complete list of the 50 comment letters categorized by stakeholder group and region.

4. The Task Force has carefully reviewed and analyzed all respondents' comments by question and has prepared and developed proposed revisions to the ED text in light of the feedback from ED respondents (see **Agenda Item 8-C** *Analysis of Respondents Views on ED, Summary of Significant ED Comments and Task Force Responses*; and **Agenda Item 8-B** *Proposed Revised Text (Mark-up from ED)).*

Interactions with the Technology Working Group

5. The Task Force met with the IESBA Technology Working Group to discuss the insights and recommendations contained in its draft Phase 2 Final Report. As appropriate, the Task Force has taken into account such insights and recommendations within the context of its analysis of comment letters received on the Technology ED.

III. Overview of ED Comments, Significant Issues Raised and Task Force Responses

6. On balance, respondents across stakeholder groups and regions expressed clear support for the proposed technology-related revisions to the Code. In support of the proposals, respondents

generally provided many suggestions to refine the proposed revisions or highlighted areas where in their view clarification is warranted to enhance the guidance.

7. Six significant issues were identified by the Task Force, which will impact how the revisions to the ED are progressed:

   - Professional Skills (Section 113).
   - Confidentiality (Section 114).
   - Complex Circumstances (Section 120).
   - Use of Technology (Sections 200, 220, 300 and 320).
   - Close Business Relationships (Section 520).
   - Hosting (Subsection 606).

   These are discussed further below.

A. Professional Skills (Section 113)

8. The ED proposed the addition of "interpersonal, communication and organizational skills" in paragraph 113.1 A1 to emphasize the professional skills that professional accountants (PAs) need. The Task Force noted fairly reserved support for the proposal. While respondents supported the proposal and acknowledged the importance of such skills, some respondents did not support[1] or expressed reservations.[2] Specifically, these respondents commented that the proposal:

   - Appears generic and not technology specific.[3] It was noted that the need for such skills has always existed, even before technology was considered.[4]
   - Involves significant judgment and would result in inconsistent application in practice. Among those who expressed that view, there was a concern that the proposals might create a possible misconception that compliance with the Code means all PAs need to be "extroverts," and that gauging the degree of competency in these skills is often a matter of personal opinion.[5]
   - Should recognize that the "soft skills" that each PA should possess is different and subject to, for example, their roles (PAs in business or in public practice) and capacity (junior PAs or senior PAs). PAs should have the communication skills which are appropriate to the tasks that they are actually performing, and that there should be effective two-way communication between the team (as a whole) and the client.[6]
   - Infers that an apparent lack of "interpersonal, communication and organizational skills" might be considered an ethical violation, as opposed to being important in the context of the realities

---

1 **PAOs:** AICPA, CPAA, IDW; **Firms:** KPMG

2 **Regulator:** IRBA; **PAOs:** ICAEW; **Firms:** DTTL, PwC; **Others:** IFAC SMPAG, MB

3 **Regulators:** IFIAR, UKFRC; **Independent NSS:** APESB; **PAOs:** CAANZ-ACCA, FACPCE

4 **Firms:** PwC

5 **Regulators:** IRBA, IFIAR; **PAOs:** MIA

6 **PAOs:** HKICPA, ICAEW, SCAAK

of practice.[7] Accordingly, a question about whether such "soft skills' are relevant in an ethics code.

- Might have a discriminatory effect on neurodiverse individuals, or inadvertently create barriers to entry for the profession.[8]

9. Respondents also suggested other skills necessary in the digital age. For example, "innovative thought leadership, adaptability, initiative, responsiveness, change management, managing technological disruption and rapidly evolving work practices" [9] and those skills pertaining to "information and communications technologies" contained in the International Education Standards (IES).[10]

10. Finally, it was suggested that the text should make it clear that such soft skills are not a complete list, by emphasizing that they are a part of professional skills[11] or rather than highlighting just a few soft skills, to acknowledge the broader requirements for PAs such as "technical competence", "professional skills", "professional values, ethics and attitudes."[12]

Task Force Response

11. The Task Force has developed revisions to the ED which considered the concerns raised by respondents. The revisions have removed sub-bullet (b) from ED paragraph 113.1 A1 given the "luke-warm" support for its inclusion, and instead introduced a new paragraph 113.1 A2 (see **Agenda Item 8-B**), intended to:

- Reflect scalability in the level of, and type of, skills needed to perform an activity competently.
- Emphasize that the soft skills highlighted are examples, and not a complete list.
- Highlight that technology-related knowledge is also relevant to professional competence in the digital age.

12. In developing the revisions, the Task Force considered referring to other soft skills that a respondent considered relevant in the digital age such as "innovative thought leadership, etc." but noted such elaboration is better positioned in non-authoritative guidance.[13] The Task Force also considered including broader categories of skills such as "technical competence", "professional skills", "professional values, ethics and attitudes" but noted that the extant Code, i.e. paragraphs 100.2 and R113.1, already outline such expectations of PAs.

13. Finally, the Task Force also considered an alternative approach to addressing the concerns raised by respondents. For example, to revise ED paragraph 113.1 A1 as follows:

113.1 A1 Serving clients and employing organizations with professional

---

7 **Firms:** DTTL, PwC; **Others:** IFAC SMPAG, MB

8 **PAOs:** AICPA, ICAEW; **Firms:** DTTL; **Others:** IFAC SMPAG, MB

9 **PAOs:** CAANZ-ACCA

10 **PAO:** CPAC

11 **PAOs:** CPAA

12 **Firms:** BDO

13 See, for example, thought leadership developed by CPA Canada, ICAS and IFAC (April 2022): *Mindset and Enabling Skills of Professional Accountants*

competence ~~requires~~ includes:

(a) ~~The exercise of~~ Exercising sound judgment in applying professional knowledge and skills; and

(b) ~~The application of~~ Applying interpersonal, communication and organizational skills.

The professional knowledge and skills necessary to perform professional activities with professional competence vary depending on the nature of the activities being undertaken. Activities that involve technology might require knowledge of a particular technology and its operation.

However, the Task Force did not proceed with this alternative approach because it still elevates the interpersonal skills into a necessity for acting with professional competence rather than emphasizing the differing level of need for such skills in certain types of activities. Accordingly, the Task Force view is that the revised ED paragraph 113.1 A1 and new paragraph 113.1 A2 in **Agenda Item 8-B** appropriately address the respondents' comments.

B. Confidentiality (Section 114)

14. The ED introduced an explicit prompt for PAs to secure confidential information in the course of the entire data governance cycle (i.e., from data generation or collection through to its use, transfer, storage, dissemination and lawful destruction) in ED paragraph 114.1 A1. Respondents expressed broad support for the proposal with some suggestions for further guidance or clarifications, including to provide:

- Additional material to address the expectations of a PA in scenarios where the information is unlawfully disclosed.[14]
- Clarity whether the provisions of Section 114 extend to the use of data for AI systems training or would prohibit the use of data that had been anonymized. It was observed that currently, the presumption of confidentiality has the effect of making firms wary of seeking consent, even for the use of pseudonymized data for collaborative research. As such, guidance that this would be permissible (given appropriate safeguards) would be welcome and help with cross-industry activities to create new technology-focused quality norms.[15]
- Clarity on what is expected of a PA to "secure" confidential information.[16]

15. The ED also included a new definition of "Confidential Information" in the Glossary (i.e., information that is not in the public domain). Respondents generally supported the definition but requested further clarity. A few respondents expressed reservations.[17] Two respondents believe "privacy" should be incorporated into the provisions.[18] The areas where further clarity was requested or reservations expressed, included:

---

[14] **Regulators:** IRBA

[15] **PAOs:** ICAEW

[16] **Regulators:** CEAOB, IAASA, IOSCO

[17] **PAOs:** CPAC, ICAEW; **Firms:** PwC

[18] **Regulators:** UKFRC; **PAOs:** ICAN

- Concern that the wording could be misinterpreted to mean that where another party does put information in the public domain (including with deliberate intent, i.e., unlawful disclosure), then the ethical principle of confidentiality would no longer apply.[19]
- Clarifying how the definition would interact with local laws and regulations (including those relating to privacy).[20]
- The term "public domain" because the term is not easily translated and is most usually associated with intellectual property rights.[21]
- The scope of confidential information. For example, whether it includes email addresses or personal information acquired from long association with a client obtained at social gatherings which may or may not be found via search engines online.[22]

16. Finally, it was also highlighted that complying with the principle of confidentiality includes consideration of the internal control environment of the PA's employing organization and often includes a sharing of such responsibility with other employees (including other PAs in business).[23] For example, while audit juniors can be held responsible for client information that comes to them during their work, they cannot be held responsible for the lawful destruction of that information (i.e., the routine destruction of emails from the firm's IT systems) as that will be undertaken in accordance with the firm's policy which is beyond their sphere of influence.[24] Along a similar vein, there were general questions about how PAs might apply the ED proposals in Parts 1 to 2 of the Code since they often involve PAs working closely with others within their employing organizations or firms (i.e., IT teams) on matters relating to the use of technology and data governance.[25]

Task Force Response

17. To address the comments raised by respondents, the Task Force developed new provisions:

    - A requirement for PAs to maintain confidentiality even if they are aware that confidential information has been improperly disclosed. (Paragraph R114.1(h) of **Agenda Item 8-B**).

      The Task Force is of the view that this concept is also relevant to client information obtained during social gatherings in the course of professional and business relationships. As part of applying the conceptual framework, a PA should exercise professional judgment and use the reasonable and informed third party test when identifying, evaluating and addressing threats to the fundamental principle of Confidentiality.
    - A prompt for PAs to consider any applicable law or regulation (including those governing privacy) in a jurisdiction where disclosure might take place. (Paragraph 114.1 A3 last bullet of **Agenda Item 8-B**).

---

19 **Regulator:** IRBA; **PAO:** ICAEW

20 **Firms:** PwC, PP

21 **PAOs:** HKICPA, CPAC

22 **PAOs:** AICPA, HKICPA, ICPAU, MIA; **Firms:** BDO

23 **Regulators:** IOSCO

24 **PAOs:** ICAS

25 **PAOs:** SCAAK; **Others:** IFAC SMPAG

This prompt emphasizes the expectation for a PA to consider relevant privacy laws or regulations when disclosing or using information. It further supplements the Code's overriding provision pertaining to a PA's obligations in respect of complying with the Code's provisions and those of local laws and regulations as set out in paragraphs R100.7 to 100.7 A1 of the Code: *"…some jurisdictions might have provisions that differ from or go beyond those set out in the Code," and "accountants in those jurisdictions need to be aware of those differences and comply with the more stringent provisions unless prohibited by law or regulation*."

- Additional material which outlines factors to be considered when providing confidential information with the consent of the provider of the information for use by third parties, and examples of circumstances when such provision might be appropriate are set out in paragraph 114.1 A4 of **Agenda Item 8-B**.

  The Task Force notes that the core concept of this type of disclosure is already catered for in extant paragraph 114.1 A2(b) where *"disclosure is permitted by law and is authorized by the client or the employing organization,"* and extant paragraph 114.1 A3, which has the factors to consider in deciding whether to disclose or use such information. The additional material has been designed to build upon such extant paragraphs to provide further guidance for PAs, recognizing that the use of data for training, research and development is not uncommon and becoming increasingly necessary in the digital age.

  The Task Force will consider drafting refinements and terminology alignment, i.e., use of "consent" and "authorize," after considering directional input from IESBA at its September meeting.

18. Responsive to respondents' requests for clarity, the Task Force has replaced the terms:

    - "Secure" in ED paragraph 114.1 A1 with "protect the confidentiality of" in order to better outline the expectation of a PA to take appropriate action to protect the confidentiality of information. (Paragraph 114.1 A1 of **Agenda Item 8-B**)
    - "Public domain" in the ED glossary definition of Confidential Information with "is not publicly available" to avoid association with intellectual property rights.

19. The Task Force acknowledges the observations that a PA's ability to comply with the provisions also depends on the employing organization's internal controls as well as the PA's position in the employing organization. The revised proposals set out in **Agenda Item 8-B** bring into consideration the employing organization's overall approach to technology issues. In particular:

    - Paragraphs 200.7 A4 and 300.7 A6 recognizes a PA's evaluation of the level of a threat associated with the use of technology might also be impacted by the work environment within the employing organization and its operating environment (such as the level of corporate oversight and internal controls over the technology).
    - Paragraphs 220.8 A1 and 320.11 A1 (6th and 7th bullets) highlights that oversight of the technology and the relevant controls relating to the use of technology within the employing organization or firm, are among the factors to consider when a PA intends to use the output of technology.
    - Paragraphs 220.9 A1 and 320.12 A1 recognizes that a PA's position in the employing organization or firm will impact his/her ability to obtain information in relation to the factors required to determine whether to use the work of others or the output of technology.

Extant paragraphs R220.7 to 220.7 A1 and R320.10 to 320.10 A1 are also relevant to a PA's use of the work of others or experts, for example, including IT teams or IT experts with an employing organization or firm.

C. Complex Circumstances (Section 120)

20. The ED included proposed guidance to explain the relevant facts and circumstances that give rise to complex circumstances and highlighted how a PA might manage the resulting challenges. Support was mixed for these proposals. While some respondents supported the proposals; some respondents did not support[26] or expressed reservations.[27]

21. In particular, some respondents[28] questioned whether the guidance is necessary in the Code. It was pointed out that complying with the fundamental principle of professional competence and due care does not require a distinction between complicated and complex matters, since in the case of both the PA is required to attain and maintain the professional knowledge and skills that are necessary to provide a competent professional service.[29] Further, the identification and managing of such circumstances are already expected of PAs in complying with the letter and spirit of the Code,[30] and that the proposed guidance would not change the threats and safeguard approach.[31] Accordingly, clarifications were requested on whether the addition of this material changes how a PA applies the:

- Conceptual framework (i.e., threats and safeguards approach).[32]
- Requirement in extant paragraph R120.9 (i.e., consideration of new information or changes in facts and circumstances).[33]

22. Some respondents[34] commented that the guidance is vague and will result in inconsistent application as it relies heavily on judgment. For example, a provision for doubtful debts may involve uncertainties and multiple variables and assumptions but would normally not be considered as complex.[35] In this regard, there was a suggestion to clarify that circumstances may not rise to the level of "complex" even if they involve both elements that are uncertain, and multiple variables and assumptions.[36] It was also noted that complexity may, to some degree, always exist because it is a relative term which is open to interpretation depending on the individual's background, skills, and experience.[37]

23. Respondents who generally viewed complexity to be at one end of the spectrum of 'complicated' and

---

26 **PAOs:** AICPA, IDW, ISCA; **Firms:** EY, GTIL, KPMG, PP, PwC; **Others:** MB

27 **PAOs:** CPAA, ICAEW, MIA; **Firms:** BDO, DTTL; **Others:** IFAC SMPAG

28 **PAOs:** IDW, ISCA, MIA; **Firms:** BDO, DTTL, GTIL; **Others:** IFAC SMPAG, MB

29 **Firms:** EY

30 **PAOs:** ISCA

31 **PAOs:** MIA; **Others:** IFAC SMPAG

32 **PAOs:** MIA

33 **Firms:** DTTL

34 **Independent NSS:** NZAuASB; **PAOs:** AICPA; **Firms:** BDO, DTTL, PP; **Others:** IFAC SMPAG

35 **Regulators:** CEAOB, IAASA

36 **Regulator:** IOSCO

37 **Regulators:** IRBA; **PAOs:** MIA; **Firms:** BDO

already addressed in the Code's conceptual framework suggested that:

- The underlying message be simplified to "assess the potential risk profile of the work to be undertaken, know your capabilities, and do not take on work that you do not understand" - which would then tie in with the need for PAs to able to understand and be able to explain the data behind automated decision making. [38]
- The concept of "complexity" be aligned with how it is addressed in ISA 315 (Revised) *Identifying and Assessing the Risks of Material Misstatement* which includes "complexity" as one of the "inherent risk factors."[39] This would then encourage a greater degree of convergence between the approaches in the Code and the ISAs.
- The notion of complexity be incorporated as a factor to be considered when evaluating threats to compliance with the fundamental principles[40] or into application material addressing actions that might be taken to manage other circumstances which is already included in the conceptual framework.[41]

24. Other respondents supportive of the proposals provided suggestions including:

- The incorporation of examples of complex matters in the Code (such as those noted in paragraph 23 of the explanatory memorandum).[42]
- The inclusion of material explaining the distinction between 'complex' and 'complicated' in the Code as PAs might not be aware of this if they are not familiar with the thought leadership paper titled *"*Complexity and the professional accountant: Practical guidance for ethical decision-making*."*[43]
- The inclusion of other factors to manage complexity in the proposals, such as documenting the uncertain elements, multiple variables, and assumptions and how they are interconnected or interdependent[44] and hiring a PA who has a broad range of relevant skills, knowledge and experience in both accounting and the technology.[45]

Task Force Response

25. On balance, given the qualified support for the provisions relating to complex circumstances and respondents varied understanding of the term "complex," the Task Force considered that there is benefit in relocating the application material to follow extant paragraphs 120.5 A4 and A5 which focus on the exercise of professional judgment. By adopting such an approach, the Task Force aims to

[38] **PAOs:** ICAEW

[39] **Regulators:** UKFRC

[40] **Firms:** KPMG

[41] **Firms:** PwC

[42] **Regulators:** IRBA; **Independent NSS:** APESB,

[43] **PAOs:** AIA, ICAS

[44] **Independent NSS:** APESB

[45] **PAOs:** JICPA

avoid:

- The criticism that this issue is merely an extension of complicated circumstances and already addressed under the Conceptual Framework.
- Practical application issues arising from a difference in approach to that taken by the IAASB.
- The criticism that the current provisions are general and vague.

The Task Force also enhanced the drafting of such material so that the average PA can more easily understand and apply it in practice, see paragraph 120.5 A6 of **Agenda Item 8-B**. The factors for managing complexity are fundamentally unchanged apart from the addition of a new factor: "analyzing, and investigating, as relevant, any uncertain elements, the multiple variables and assumptions and how they are connected or interdependent," see paragraph 120.5 A7 of **Agenda Item 8-B**.

26. The Task Force considered whether further documentation considerations should be included in such material, or whether references to PAs having relevant training and experience are appropriate; but determined that the current provisions related to these matters in the extant Code are sufficient.

27. Finally, the Task Force considered whether it is appropriate to build in some of the thinking in explanatory memorandum paragraph 23 but noted that it is too detailed for a principles-based Code, and more appropriate for non-authoritative guidance, such as the thought leadership paper already issued.

D. Use of Technology (Sections 200, 220, 300 and 320)

28. The ED introduced considerations to help in identifying threats that might arise when PAs rely upon the output from technology (ED paragraphs 200.6 A2 and 300.6 A2). Respondents were generally supportive, with a few respondents who expressed reservations.[46] One stakeholder did not support the proposals because they do not contain sufficient information and guidance for PAs.[47] The key comments raised were:

- That the considerations outlined in ED paragraphs 200.6 A2 and 300.6 A2 should be linked to specific threats to compliance with the fundamental principles[48] and that a sub-heading – "Identifying threats associated with the use of technology" – should be added.[49]
- Whether it is reasonable to expect a PA to have sufficient expertise or understanding to be able to use and explain the technology. In this regard it was suggested that access to an expert with such expertise or understanding should be regarded as equivalent. [50]
- That the meaning of the penultimate bullet "whether technology incorporates expertise or judgements of the accountant or the employing organization/ firm" requires clarification[51] In this regard, there were requests to address scenarios such as where the PA licenses technology

[46] **PAOs:** ASSIREVI, CNCC, ICAEW, ICAS, KICPA; **Firms:** DTTL

[47] **PAOs:** SAICA

[48] **Regulators:** IRBA, IFIAR; **PAOs:** AICPA, CPAC, MIA, SAICA; **Firms:** BDO, KPMG

[49] **Firms:** RSM

[50] **Regulators:** UKFRC, IRBA, IFIAR; **PAOs:** HKICPA; **Firms:** MNP

[51] **Independent NSS:** APESB; **PAOs:** ASSIREVI; **Firms:** DTTL, GTIL; PwC; **Other:** MB

to use versus where the PA develops and uses technology,[52] and whether placing reliance on in-house technology rather than on third-party technology increases or diminishes the threat.[53]

- That a number of additional considerations relevant to a PA's identification of threats to the fundamental principles should be included. For example:
  - The source and appropriateness of the inputs to the technology (i.e., sufficiency of data quality and programming underpinning the technology).[54]
  - The level of sophistication or maturity of the technology as it will impact the availability of information about how the technology functions or how widespread (i.e., commonly accepted) the technology is.[55]
  - Expectations in relation to documentation.[56]
  - Specific issues to be considered by PAs in relation to the training of AI systems.[57]
- Safeguards for the threats should be identified and added, such as third-party certifications (including independent governance or accreditation processes to assess the quality and functionality of the technology), compliance with recognized technology standards and periodic reviews.[58]

29. The ED also introduced examples of factors for PAs to consider in determining whether reliance on or use of the output of technology is reasonable or appropriate for the intended purpose (ED paragraphs 220.7 A2 and 320.10 A2). Respondents were generally supportive, although a few respondents expressed reservations[59] or did not support the proposals.[60] Regulators[61] that did not support the proposals suggested that:

- The challenges PAs face when using technology should be presented in a section separate from *Using the Work of an Expert* because the conceptual considerations differ. When using the work of an expert, a PA is relying on an individual or organization's intrinsic expertise in relation to a specific subject matter, their experience, skills, qualifications, and judgements to assist in their work, and drawing conclusions based on reports or other works prepared by the expert. However, when using technology, the PA needs to understand the data being used, the complexity of the relationships present and enough of the working of the tools to ensure that the PA is meeting their professional competence and due care obligations.

---

52 **Firms:** PwC

53 **Firms:** DTTL

54 **Regulators:** CEAOB, IAASA, UKFRC; **PAOs:** CPAA, ICAEW

55 **PAOs:** CPAA; **Firms:** EY

56 **PAOs:** HKICPA, MIA

57 **PAOs:** ICAEW

58 **Regulators:** BAOA, UKFRC, IRBA

59 **Regulators:** IRBA; **Others:** IFAC SMPAG, MB

60 **Regulators:** IFIAR, UKFRC; **PAOs:** SAICA

61 **Regulators:** IFIAR, UKFRC

- Emphasis should be on the whole process for making use of a technological resource, rather than on the use of the output of the technology.

30. In addition, ED respondents requested clarification or made suggestions for the incorporation of additional factors, such as:

    - Whether appropriate user management processes and controls are in place – for example oversight and authorization of roles that users are assigned in the system and super users.[62]
    - Whether an organization's general and application controls related to the technology are effective.[63]
    - Clarify how the reputation of a software developer is assessed (i.e., reputation could be subjective and unreliable without further due diligence) and how this factor would impact the PA's considerations when it is not possible to assess their reputation, especially when it involves emerging technology.[64]
    - Emphasize the accountability of PAs – which is particularly relevant where the decision-making is automated - by adding consideration of the "decisions made by individuals relating to the operation of the technology."[65]
    - Recognize that a firm or employing organization's oversight of technology will be different depending on whether the technology is developed in-house as opposed to having been purchased from third parties.[66] For example, a firm or employing organization will not be able to review the source code of technology purchased from third parties as that is proprietary.[67] The emphasis should be about assessing the vendors and whether they have provided sufficient information for PAs to have oversight of the third-party technology.[68]

Task Force Response

31. The Task Force has recognized and addressed the key feedback, drafting suggestions and concerns in paragraphs 200.6 A2, 220.8 A1, 300.6 A2 and 320.11 A1 of **Agenda Item 8-B**. Additionally, paragraphs 200.7 A4 and 300.7 A6 have been developed to provide examples of where a PA's evaluation of the level of a threat associated with the use of technology might also be impacted by the work environment within the employing organization and its operating environment.

32. The Task Force view is that the existing provisions in relation to the documentation of the exercise of professional judgement when complying with the fundamental principles are sufficient. Furthermore, the need for documentation is not limited to the use of technology, and the IESBA has determined in its 2019-2023 Strategy Work Plan that a potential project related to reconsidering the documentation provisions in the Code was not a high priority at that time.

---

62 **Regulators:** CEAOB, IOSCO

63 **PAOs:** IDW; **Firms:** RSM

64 **Regulators:** IRBA; **PAOs:** HKICPA, MIA; **Firms:** BDO

65 **PAOs:** ICAS

66 **Firms:** PwC

67 **Others:** MB

68 **Others:** IFAC SMPAG

33. With respect to the suggestion that additional guidance should be included to address the specific issues to be considered by PAs in relation to the training of AI systems, the Task Force is of the view that such considerations are too specific for the Code and might create a precedent of including specific guidance for each type of technology a PA might encounter. However, the Task Force agrees that there is benefit to developing guidance in this area and notes that the Technology Working Group's draft Phase 2 Final Report highlights considerations for PAs in relation to the use or development of AI systems.

34. The Task Force considered the appropriateness of adding scenarios to illustrate the circumstances in which using in-house technology and third-party technology increases or diminishes a threat to compliance with the fundamental principles. However, the Task Force concluded that it would be impossible to do so since each situation would depend on the specific facts and circumstances.

35. As regards the concerns relating to the focus on the "output of the technology," the Task Force noted that such phrase does not mean that the proposals do not consider the whole process for making use of a technological resource. In this regard, the Task Force noted that the following factors in paragraphs 220.8 A1 and 320.11 A1 of **Agenda Item 8-B** are relevant:

- The employing organization's or firm's oversight of the design, development, implementation, operation, maintenance, monitoring, updating or upgrading of the technology.
- The controls relating to the use of the technology, including procedures for authorizing user access to the technology and overseeing such use.
- The appropriateness of the inputs to the technology, including data and any related decisions, and decisions made by individuals in the course of using the technology.

36. Finally, the Task Force is of the view that how a firm or employing organization exercises "oversight" for in-house versus third-party technology will indeed differ depending on the facts and circumstances and that such differences in approach are not limited to the use of technology.

E. Close Business Relationships (Section 520)

37. The ED included a signpost in Section 520 *Business Relationships* which prompted firms to consider the relevance of the non-assurance services (NAS) provisions in Section 600 when technology is provided, sold, resold[69] or licensed by a firm or a network firm to an audit client (ED paragraphs 600.6 and 520.7 A1).

38. Respondents were mainly supportive, although a few respondents did not support[70] or expressed reservations.[71] In particular, concerns were expressed that the interaction between the NAS and business relationship provisions in the Code, which cover very different relationships, will become unclear.[72] There were also concerns and requests for clarity in relation to the resale of third-party

---

[69] The IESBA noted that reselling could consist of a "pass-through" of products developed by third parties to audit clients with no other services attached or could also combine ancillary/ associated services provided by the firm or a network firm with the product being resold. In either case, firms are prompted to consider whether the NAS provisions are relevant to the facts and circumstances of the reselling arrangement.

[70] **PAOs:** ISCA; **Firms:** DTTL, KPMG

[71] **PAOs:** CPAA

[72] **Firms:** DTTL, KPMG

technology in "pass-through" situations, where it may not follow that a NAS would be provided requiring assessment under Section 600.[73]

39. It was also suggested that additional clarity on "indirect" provision of services be provided.[74] This respondent observed a number of scenarios where firms have developed software for non-audit clients, who subsequently use this software to provide a service to those firms' audit clients.

40. The ED provided an example of a close business relationship arising from the provision of technology. There was general support for the inclusion of such an example, and suggestions to include others such as:

    - Products or solutions related to technology which one or both parties use for their internal purposes.[75]
    - That contained in paragraph 40 of the explanatory memorandum where firms are licensing software: (a) to their audit clients, who are in turn directly utilizing the technology in the delivery of services to their own customers/clients; or (b) from an audit client and directly using the technology in the delivery of services to their clients.[76]

    There were also calls to include a general principle for the identification or assessment of "close business relationships", recognizing that the examples provided cannot cover all scenarios.[77]

Task Force Response

41. The Task Force noted the disagreement by a few respondents with respect to including a signpost to Section 600 within ED paragraph 520.7 A1. However, the Task Force is of the view that this signpost is necessary based on the results of the survey titled "The Impact of Technology on Auditor Independence" which indicated that 24% of respondents did not think that NAS provisions are relevant when a firm sells or licenses technology that performs a NAS. The Task Force also resolved to include an explanation in the Basis for Conclusions to make it clear that whether a "pass-through" reselling arrangement situation is a NAS depends on the facts and circumstances.

42. The Task Force has addressed situations identified by respondents where the provision of technology to audit clients or third parties might give rise to a close business relationship. Specifically, it has:

    - Expanded the signpost contained in ED paragraph 520.7 A1 to include "indirect" services, where firms have developed software for non-audit clients, who subsequently use this software to provide a service to the firm's audit clients. (Paragraphs 520.7 A1(b) and 600.6 of **Agenda Item 8-B**).
    - Highlighted that arrangements under which the firm or a network firm licenses products or solutions to or from a client might create a close business relationship. (Paragraph 520.3 A3 of **Agenda Item 8-B**).

      The Task Force acknowledges the varied nature of these licensing arrangements and how the

[73] **PAOs:** AICPA; **Firms:** BDO, DTTL, MNP

[74] **Regulator:** UKFRC

[75] **Regulator:** CEAOB

[76] **PAOs:** ICAS

[77] **PAOs:** HKICPA

technology is used, and also observes that there are a number of instances where such arrangements are purchases in the ordinary course of business (for example, a firm licensing from an audit client products or solutions which comprise office software). Accordingly, the Task Force explicitly emphasized that such arrangements "might create" a close business relationship since it depends on the specific facts and circumstances.

F. Hosting (Subsection 606)

43. The ED introduced a prohibition on services relating to the hosting (directly or indirectly) of an audit client's data. Respondents generally supported the proposal, although a few respondents did not support[78] or expressed reservations.[79]

44. The comments raised (whether in support for further clarification or as a reservation or concern) mainly related to the potential broad, and hence unclear, interpretation of the prohibition. For example, whether:

- The phrase "services in relation to hosting" should be interpreted to include a wide range of services including, vendor selection services for a hosting platform, providing benchmarks on capacity requirements, providing the cloud infrastructure service itself, or delivering a service or solution via the cloud.[80]
- The scope of the prohibition is intended to cover:
  - Portals to transfer client data to support deliverables as required under professional standards where the client is responsible for downloading any deliverables or other records upon completion of the service.[81] In this regard, it was suggested that the term "transmission" be included in ED paragraph 606.3 A2 to clarify that it does not cover such situations.[82]
  - Hosting of any data irrespective of whether it is the client's source or primary data, or a copy of it.[83]
- Consideration should be given to all types of data being hosted, the method of hosting, the purpose of the hosting and whether management responsibility is being assumed.[84]
- Whether the phrase "directly or indirectly" should be explained in the Code (e.g., as it was in the explanatory memorandum (paragraph 52) – either directly on internal servers or indirectly on a cloud provider's servers.[85]

---

78 **Firms:** BDO, DTTL

79 **PAOs:** CPAA, IDW; **Firms:** MNP

80 **Firms:** EY, DTTL

81 **Firms:** GTIL

82 **Others:** IFAC SMPAG

83 **Firms:** DTTL

84 **PAOs:** CAANZ-ACCA**,** MIA; **Firms:** BDO, DTTL

85 **PAOs:** AICPA

Task Force Response

45. The Task Force has considered the comments and revised the material in relation to hosting, see paragraph 606.3 A1 of **Agenda Item 8-B**. In particular, it replaced the phrase "services in relation to hosting" in the lead-in with "stores data or manages" to be more specific as to the type of hosting services covered by the prohibition. Furthermore, it has introduced sub-bullets (a) to (c) in order to provide examples of when a specific method or purpose of hosting would involve an assumption of management responsibility, and to clarify that it does not cover the hosting of all data (i.e., including copies of client data).

46. Additionally, the term "transmission" has been added to ED paragraph 606.3 A2 to highlight that portals for transferring information in the course of providing a permissible service are not prohibited.

47. The Task Force will explain the concept of directly or indirectly in the Basis for Conclusions.

IV. Matters for IESBA Consideration

48. During the September 2022 meeting, the Task Force[86] Chair will walk-through the key issues and preliminary Task Force Responses, drawing from material in **Agenda Items 8-A and 8-B**. In particular, IESBA members will be asked to consider and react to the following:

    (a) The overview of the significant issues raised by ED respondents; and

    (b) The Task Force's preliminary thinking on significant issues – as that will impact how the revisions to the ED will be progressed.

V. Next Steps

49. The Task Force plans to meet during the IESBA's September 2022 meeting week to consider input received in refining the revisions to the ED.

Materials for Discussion

Agenda Item 8-A	Technology Project – Presentation Slides *(Significant Issues and Task Force Responses)*
Agenda Item 8-B	Proposed Revised Text *(Mark-up from ED)*

[86] Task Force Members comprise:

- Rich Huesken, Chair and IESBA Member
- Hironori Fukukawa, IESBA Member
- Luigi Nisoli, IESBA Member
- Greg Driscoll, IESBA Technical Advisor
- James Barbour, former IESBA Technical Advisor

Mr. Richard Fleck, who is the Non-assurance Services Task Force Chair and former IESBA Deputy Chair, provides advice and support to the Task Force.

Agenda Item 8-C	Analysis of Respondents Views on ED, Summary of Significant ED Comments and Task Force Responses
Agenda Item 8-D	Supplementary Material – Compilation of ED Comments *(General and by Question)*
Agenda Item 8-E	Reference Material – Proposed Revised Text *(Mark-up from Extant)*
Agenda Item 8-F	Reference Material – Proposed Revised Text *(Clean)*

Appendix 1

List of Respondents to the Technology ED

Note: Members of the Monitoring Group are shown in **bold** below.

#	Abbrev.	Respondent (50)	Region
Regulators and Oversight Authorities, Including MG members (8)			
1.	BAOA	Botswana Accountancy Oversight Authority	AP
2.	CEOAB	Committee of European Auditing Oversight Bodies	EU
3.	IAASA	Irish Auditing & Accounting Supervisory Authority	EU
4.	IRBA	Independent Regulatory Board for Auditors	MEA
5.	**IFIAR**	**International Forum of Independent Audit Regulators**	**GLOBAL**
6.	**IOSCO**	**International Organization of Securities Commissions**	**GLOBAL**
7.	NASBA	National Association of State Boards of Accountancy (US)	NA
8.	UKFRC	United Kingdom Financial Reporting Council	EU
Independent[87] National Standard Setters (2)			
9.	APESB	Accounting Professional & Ethical Standards Board (Australia)	AP
10.	NZAuASB	New-Zealand Auditing & Assurance Standard Board	AP
Professional Accountancy Organizations (PAOs) (27) [88]			
11.	AAT	Association of Accounting Technicians	EU
12.	ACCA—CAANZ$^{\delta}$	Joint Submission: Association of Chartered Certified Accountants—Chartered Accountants Australia and New Zealand	GLOBAL

[87] NSS that have a mandate to set national ethics standards, including independence requirements, in their jurisdictions and which do not belong to PAOs are categorized as "Independent National Standard Setters."

The IESBA has a liaison relationship with a group of NSS (both independent NSS and organizations that hold dual NSS-PAO roles) that share the common goal of promulgating high-quality ethics standards, including independence requirements, and seeking convergence for those standards. Participating jurisdictions include Australia, Brazil, Canada, China, France, Germany, Hong Kong SAR, India, Japan, the Netherlands, New Zealand, Russian Federation, South Africa, the UK, and the US.

[88] For purposes of this categorization, a PAO is a member organization of professional accountants, of firms, or of other PAOs. PAOs include but are not limited to IFAC member bodies. **PAOs that have full, partial or shared responsibility for setting national ethics standards, including independence requirements, in their jurisdictions are indicated with a "δ".**

#	Abbrev.	Respondent (50)	Region
13.	AIA	Association of International Accountants	GLOBAL
14.	AICPA[δ]	American Institute of Certified Public Accountants Professional Ethics Executive Committee	NA
15.	ASSIREVI	Association of the Italian Audit Firms	EU
16.	BICA[δ]	Botswana Institute of Chartered Accountants	AP
17.	CNCC[δ]	Compagnie Nationale des Commissaires aux Comptes	EU
18.	CPAA	CPA Australia	AP
19.	CPAC[δ]	Chartered Professional Accountants Canada Public Trust Committee	NA
20.	FACPCE	Federación Argentina de Consejos Profesionales de Ciencias Económicas	SA
21.	HKCIPA[δ]	Hong Kong Institute of Certified Public Accountants	AP
22.	IBRACON	Instituto dos Auditores Independentes do Brasil	SA
23.	ICAEW[δ]	Institute of Chartered Accountants in England and Wales	EU
24.	ICAI[δ]	The Institute of Chartered Accountants of India	AP
25.	ICAN	The Institute of Chartered Accountants of Nigeria	AP
26.	ICAS[δ]	The Institute of Chartered Accountants of Scotland	EU
27.	ICPAU[δ]	Institute of Certified Public Accountants of Uganda	MEA
28.	IDW[δ]	Institute der Wirtschaftsprüfer (Germany)	EU
29.	ISCA[δ]	Institute of Singapore Chartered Accountants	AP
30.	JICPA[δ]	Japanese Institute of Certified Public Accountants	AP
31.	KICPA[δ]	Korean Institute of Certified Public Accountants	AP
32.	MIA	Malta Institute of Accountants	EU
33.	MIA[δ]	Malaysian Institute of Accountants	AP
34.	NBA[δ]	Royal Netherlands Institute of Chartered Accountants	EU

#	Abbrev.	Respondent (50)	Region
35.	SAICA$^{\delta}$	South African Institute of Chartered Accountants	MEA
36.	SCAAK	Society of Certified Accountants and Auditors of Kosovo	EU
37.	TFAC	Federation of Accounting Professions, Thailand	AP
Firms (8)[89]			
38.	BDO*	BDO International Limited	GLOBAL
39.	DTTL*	Deloitte Touch Tohmatsu Limited	GLOBAL
40.	EY*	Ernst & Young Global Limited	GLOBAL
41.	GTIL*	Grant Thornton International Ltd.	GLOBAL
42.	KPMG*	KPMG IFRG Limited	GLOBAL
43.	MNP	MNP LLP Canada	NA
44.	PWC*	PricewaterhouseCoopers International Limited	GLOBAL
45.	PP	Pitcher Partners	AP
46.	RSM*	RSM International Limited	GLOBAL
Others (4)			
47.	IFAC SMPAG	IFAC Small and Medium Practices Advisory Group (IFAC SMPAG)	GLOBAL
48.	AS	Dr. Asha Sharma	AP
49.	AFV	Álvaro Fonseca Vivas	SA
50.	MB	MindBridge	NA

[89] Forum of Firms members are indicated with a *. The Forum of Firms is an association of international networks of accounting firms that perform transnational audits.