Basis for Conclusions
Prepared by the Staff of the IESBA®
April 2023

International Ethics Standards Board for Accountants®

Technology-related Revisions to the Code

IESBA International Ethics Standards Board for Accountants®

IESBA International Ethics Standards Board for Accountants®

About the IESBA

The International Ethics Standards Board for Accountants® (IESBA®) is an independent global standard-setting board. The IESBA's mission is to serve the public interest by setting ethics standards, including auditor independence requirements, which seek to raise the bar for ethical conduct and practice for all professional accountants through a robust, globally operable *International Code of Ethics for Professional Accountants (including International Independence Standards)* (the Code).

The IESBA believes a single set of high-quality ethics standards enhances the quality and consistency of services provided by professional accountants, thus contributing to public trust and confidence in the accountancy profession. The IESBA sets its standards in the public interest with advice from the IESBA Consultative Advisory Group (CAG) and under the oversight of the Public Interest Oversight Board (PIOB).

The structures and processes that support the operations of the IESBA are facilitated by the International Foundation for Ethics and Audit™ (IFEA™).

BASIS FOR CONCLUSIONS:

TECHNOLOGY-RELATED REVISIONS TO THE CODE

CONTENTS

I. Introduction

1. The IESBA unanimously approved the technology-related revisions to the Code at its November–December 2022 meeting.

2. This Basis for Conclusions is prepared by IESBA staff and explains how the IESBA has addressed the significant matters raised on exposure and in the course of finalizing the revisions. It relates to, but does not form part of, the technology-related revisions set out in the final pronouncement.

3. The technology-related revisions are to the most current version of the Code, i.e., as contained in the 2022 edition of the Handbook of the *International Code of Ethics for Professional Accountants (including International Independence Standards)* ("extant Code") together with the approved revisions not yet effective as of December 2022 relating to the *Definitions of Listed Entity and Public Interest Entity*, and *Definition of Engagement Team and Group Audits*.

4. The technology-related revisions affect all Parts of the Code and include changes to Sections 110 (i.e., Subsections 113 and 114), 120, 200, 220, 300, 320, 400, 520, 600 (including Subsections 601 and 606), 900, 920 and 950. They also include revisions to the Glossary and conforming amendments in Sections 260 and 360 of the Code.

A. About the Technology-related Revisions

5. The revisions arising from the Role and Mindset and Non-Assurance Services (NAS) projects introduced changes to the Code relevant to technology. Building on those changes, the technology-related revisions enhance the Code's robustness and expand its relevance in an environment being reshaped by rapid technological advancements and accelerated digitalization.

6. The revisions are principles-based and apply to all technologies so as to be able to withstand, to the extent possible, the ever-evolving landscape of technology transformation. In particular, the revisions:

   - Provide guidance relevant to elements of the fundamental principles that are important for the digital age.
   - Enhance the Code's robustness in guiding the mindset and behavior of professional accountants (PAs) in business (PAIBs) and in public practice (PAPPs) as they deal with changes brought about by the use of technology.
   - Enhance the International Independence Standards (IIS) by clarifying and addressing the circumstances in which firms and network firms may or may not provide a technology-related NAS to an audit or assurance client.

II. Background

A. Development of the Project Proposal and Technology-related Revisions

7. The genesis of the technology project was a focus on developments in technology as a high priority area in the IESBA's *Strategy Work Plan 2019-2023*, consistent with strategic input from the Public Interest Oversight Board (PIOB).

8. The project proposal, approved in March 2020, was informed by the recommendations contained in the IESBA Technology Working Group's Phase 1 Report, which summarized the impact of trends and developments in artificial intelligence (AI), big data, and data analytics on the ethical behavior of PAIBs and PAPPs.

9. Since then, the IESBA's technology project was informed by:

- Technology-related feedback on the January 2020 NAS Exposure Draft.
- Feedback on two October 2020 technology surveys on the topics of "Technology and Complexity in the Professional Environment" and "The Impact of Technology on Auditor Independence."
- Stakeholder responses to the IESBA's Technology Exposure Draft (ED).
- The insights and observations of the Technology Working Group's Phase 2 fact-finding, including some of the recommendations set out in the November 2022 Phase 2 Final Report.[1]
- Targeted stakeholder input together with advice from the IESBA Consultative Advisory Group (CAG) and the IESBA–National Standard Setters (NSS) liaison group.

B. Objective of the Project

10. The objective of the project was to respond in a timely manner to the transformative effects of major trends and developments in technology on the accounting, assurance and finance functions. The public interest is served by these technology-related revisions because they will help ensure that the Code's provisions remain relevant and fit for purpose.

C. Interaction with Other IESBA Work Streams and Coordination with IAASB

IESBA Technology Working Group

11. In developing and finalizing the technology-related revisions to the Code, the IESBA considered relevant preliminary insights and observations arising in the course of the Technology Working Group's fact-finding and the final insights and recommendations in the Working Group's Phase 2 Report.

IAASB-IESBA Coordination

12. In finalizing the revisions to the ED, the IESBA continued to coordinate with the International Auditing and Assurance Standards Board (IAASB) to maintain the alignment and interoperability between the two Boards' sets of standards. Steps have, in particular, been taken to ensure that:

- The revisions preserve the existing consistency of Part 4B of the Code with the terms and concepts in the IAASB's International Standard on Assurance Engagements (ISAE) 3000 (Revised), Assurance Engagements other than Audits or Reviews of Historical Financial Information.
- The revisions with respect to the fundamental principle of confidentiality do not require conforming amendments to the IAASB's International Standard on Quality Management (ISQM) 1 Standard.[2]

---

[1] The Technology Phase 2 fact-finding aimed to identify and assess the potential impact of technology on the behavior of PAs and the relevance and applicability of the Code. Focused on the most pressing emerging, disruptive, and transformative technologies, it involved desktop research and stakeholder interviews and other outreach. The Phase 2 Final Report provides an overview of the technology landscape, as well as key themes, conclusions, insights, and recommendations for the IESBA and others.

[2] ISQM 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements*

D. Technology Exposure Draft

12. On February 18, 2022, the IESBA issued the proposed revisions to 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. 50 comment letters were received across a wide range of stakeholder groups and geographical regions. In addition to two Monitoring Group (MG)[3] members, respondents included six regulators and audit oversight bodies, 27 professional accountancy organizations (PAOs),[4] two independent NSS,[5] nine firms, and four others, including the IFAC Small and Medium Practices Advisory Group (IFAC SMP AG) and an AI software developer.

13. On balance, respondents across stakeholder groups and regions expressed clear support for the proposals. They also suggested various drafting improvements and shared some concerns and a number of other comments, including highlighting areas where in their view clarification was warranted. The significant issues and principal matters raised by respondents, and the approach taken by the IESBA in response, are discussed in Section III below.

14. In revising its proposals to address matters raised by respondents to the ED, the IESBA also took into account input from targeted outreach with representatives of the:

- IESBA CAG.
- IAASB Technology Consultative Group.
- IFIAR Standards Coordination Working Group (IFIAR SCWG).
- IOSCO Committee on Issuer Accounting, Audit and Disclosure (IOSCO Committee 1).
- Forum of Firms.

III. Significant Matters

15. Respondents raised substantive matters in relation to the following six areas, resulting in revisions to the ED:

- 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).

---

[3] The MG respondents were the International Forum of Independent Audit Regulators (IFIAR) and the International Organization of Securities Commissions (IOSCO).

[4] For purpose of analyzing its comment letters, the IESBA deems a PAO to be a member organization of professional accountants, of firms, or of other PAOs. PAOs include, but are not limited to, members of the International Federation of Accountants (IFAC). PAOs might have full, partial, or shared responsibility for setting national ethics standards, including independence requirements, in their jurisdictions.

[5] Independent NSS have a mandate to set national audit and ethics standards, including independence requirements, and do not belong to PAOs.

These are discussed further below.

A. Professional Skills (Section 113)

Technology ED

16. The ED proposed the addition of "interpersonal, communication and organizational skills" in ED paragraph 113.1 A1 to emphasize the professional skills that PAs need. The development of the proposal was informed by IFAC's International Education Standards (IESs)[6] that came into effect on January 1, 2021, and reflects the need for PAs to be skilled in information and communications technologies. Specifically, the proposal was intended to emphasize the importance of skills contained in IES 3: Professional Skills.[7]

17. The proposals in the ED reflected the IESBA's view that:

    (a) "Interpersonal, communication and organizational skills" are generally applicable in the execution of all professional activities and are not specific to technology-related circumstances; and

    (b) The extant Code (i.e., paragraph 113.1 A2) sufficiently spells out the PA's obligation to identify the applicable professional competence standards and resources in order to comply with the requirement in paragraph R113.1.

---

[6] Standards of professional competence in the IESs are made available to PAs through their PAOs, which are subject to IFAC's Statements of Membership Obligations (SMOs). SMO 2 sets out requirements for IFAC member organizations with respect to IESs for PAs and Aspiring PAs. Paragraphs 4 and 5 of SMO 2 state that:

- IFAC recognizes that its member organizations operate under different national legal and regulatory frameworks and are comprised of professionals working in different sectors of the accountancy profession. Accordingly, IFAC member organizations in different jurisdictions may have different degrees of responsibility for meeting the requirements in this SMO and should refer to the applicability framework on page 7 of the SMO Handbook.
- In accordance with the applicability framework, IFAC member organizations shall identify and undertake actions to have the IESs adopted and implemented in their jurisdictions.

[7] The level of proficiency for "Interpersonal and Communication Skills" as specified by IES 3 is for PAs to:

- Demonstrate collaboration, cooperation and teamwork when working towards organizational goals.
- Communicate clearly and concisely when presenting, discussing, and reporting in formal and informal situations.
- Demonstrate awareness of cultural and language differences in all communication.
- Apply active listening and effective interviewing techniques.
- Apply negotiation skills to reach solutions and agreements.
- Apply consultative skills to minimize or resolve conflict, solve problems, and maximize opportunities.
- Present ideas and influence others to provide support and commitment.

The level of proficiency for "Organizational Skills" as specified by IES 3 is for PAs to:

- Undertake assignments in accordance with established practices to meet prescribed deadlines.
- Review own work and that of others to determine whether it complies with the organization's quality standards.
- Apply people management skills to motivate and develop others.
- Apply delegation skills to deliver assignments.
- Apply leadership skills to influence others to work towards organizational goals.

Feedback from ED Respondents

18. On balance, respondents were generally supportive of including a reference to such skills, although some did not support it or expressed reservations. Among the substantive comments raised, it was felt that the ED proposal:

    - Appeared generic and not technology-specific.
    - Would involve significant judgment and result in inconsistent application in practice, as gauging the degree of competency in these skills is often a matter of personal opinion.
    - Should recognize that PAs should have professional skills which are commensurate with the professional activities they are actually performing, and that there should be effective two-way communication between the team (as a whole) and the client.
    - Suggested that an apparent lack of "interpersonal, communication and organizational skills" might be an ethical violation, and furthermore, might lead to a conclusion that such skills are the only professional skills necessary for a PA.
    - Might have a discriminatory effect on "neurodiverse" individuals, or inadvertently create barriers to entry for the profession.

19. It was also noted that the need for such skills has always existed, even before technology was considered.

20. Suggestions for other skills considered necessary in the digital age were provided. For example, "innovative thought leadership, adaptability, initiative, responsiveness, change management, managing technological disruption and rapidly evolving work practices" and those skills pertaining to "information and communications technologies" contained in the IESs.

IESBA Decisions

21. The IESBA made revisions to the ED to address the comments raised by respondents. ED paragraph 113.1 A1 sub-bullet (b) was withdrawn, and a new paragraph 113.1 A2 was introduced to:

    - Recognize that the professional knowledge and skills needed to perform a professional activity competently will vary depending on the nature of the activity. This concept has also been emphasized in revised paragraph 113.1 A3 (extant paragraph 113.1 A2), which states that maintaining professional competence requires a PA to have a continuing awareness and understanding of technical, professional, business and technology-related developments relevant to the professional activities undertaken. The revisions highlight that a PA should achieve a level of understanding "*relevant to the activities undertaken by the PA*."
    - Emphasize that interpersonal, communication and organizational skills are only examples of professional skills which facilitate a PA's interaction with others, and therefore are not the only skills relevant when a PA undertakes professional activities. This provision further highlights that such examples of professional skills are in addition to the application of any technical knowledge relevant to the professional activity.

22. With respect to the comment that the ED proposal was not technology-specific, the IESBA reaffirmed that the revisions are intended to apply to all circumstances, including those related to technology. The revisions will prompt, and guide, PAs to think through the level and type of professional skills and knowledge necessary to comply with paragraph R113.1 and perform a competent professional

service. This guidance is particularly relevant in relation to technology as the PA's role is constantly evolving due to, for example, the automation of routine tasks and emerging technology applications in the workplace.

23. Regarding the concern that significant judgment is involved in evaluating the degree of competency in relation to the examples of professional skills, the IESBA noted that when a PA identifies the applicable professional competence standards and resources in order to comply with R113.1, the PA might consider the IESs which contain detailed guidance regarding what a PA should be able to demonstrate to be considered to have an appropriate level of proficiency.

24. With respect to the suggestion to incorporate other skills into the Code, such as innovative thought leadership or adaptability, the IESBA considered that such detail would be more appropriate in non-authoritative guidance, which can better elaborate on how these skills are helpful in today's technology-driven world.[8]

B. Confidentiality (Section 114)

Technology ED

25. 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. It also included a new definition of "confidential information" in the Glossary (i.e., information that is not in the public domain). Refinements to modernize the language in Section 114 were also proposed in the ED, recognizing that there are currently various digital communication tools being used, and that there will continue to be the development of new communication tools in the future.

26. The IESBA regarded these ED proposals as particularly relevant in light of today's data-driven world and the ease with which data is accessible. This view was reflected in the ED approach, which established a threshold of "confidentiality" with which a PA is required to comply. This threshold includes information acquired by a PA in the course of their professional or business relationships:

    (a) In whatever capacity (including through "social" gatherings with a client or customer);

    (b) In any form or medium (e.g., including multi-media, written, electronic, visual or oral); and

    (c) Whether or not such information is already publicly available.

27. The ED also reflected the IESBA's view that the Code's fundamental principle of confidentiality is all encompassing and is intended to cover "privacy" in a principles-based manner, and that it would be inappropriate to expand on the concept of privacy in the proposed Glossary definition. This is because the concept of privacy is often covered in jurisdiction-level laws and regulations (e.g., the EU's General Data Protection Regulation), and would give rise to varying and potentially contradictory approaches to interpretation and application across different jurisdictions.

28. The overriding provisions in extant 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"*) already require a PA to comply with such national

[8] See, for example, thought leadership developed by CPA Canada, ICAS and IFAC (April 2022): *Mindset and Enabling Skills of Professional Accountants*, to which the Technology Working Group contributed.

laws and/or regulations.

Feedback from Respondents

29. Respondents broadly supported the proposed revisions to Section 114 and the Glossary definition, with comments and drafting suggestions to improve the proposed text.

30. Regarding the fundamental principle of confidentiality more generally, the following principal suggestions were raised:

- To clarify whether the fundamental principle of confidentiality continues to apply where another party puts information in the public domain (whether lawfully or unlawfully).
- To clarify whether the provisions of Section 114 would prohibit the use of data that has been anonymized (e.g., for research related to technology-focused quality norms or for the training of internal AI systems). Recommendation A of the Technology Working Group's Phase 2 Report also highlights this matter.

31. Regarding proposed ED paragraph 114.1, there was a suggestion that the Code should include material to explain what steps a PA is expected to take to "secure" confidential information.

32. Regarding the proposed Glossary definition, the principal points raised were:

- The term "public domain" might cause confusion as that term is most usually associated with intellectual property rights (i.e., copyright law).
- To clarify how the Glossary definition would interact with local laws and regulations (including those relating to privacy). In this regard, there was a view that additional guidance should be included addressing how PAs might respond to potential conflicts between local laws and regulations when undertaking cross-border engagements. In addition, a few respondents supported explicitly incorporating the term "privacy" into the Glossary definition.
- To clarify what the scope of confidential information is, for example, whether it includes email addresses or personal information acquired from long association with a client or obtained at social gatherings, which may or may not be found via search engines online.

IESBA Decisions

33. The IESBA addressed comments raised in relation to Section 114 in the context of the confidentiality concepts contained in the extant Code. Specifically, the extant Code recognizes that confidentiality serves the public interest because it facilitates the free flow of information from the PA's client or employing organization to the PA in the knowledge that the information will not be disclosed to a third party. A PA's compliance with the principle of confidentiality (i.e., duty of confidentiality as set out in the Code) is therefore based on this underlying premise.

34. Concerning the comments about when confidential information can be used or disclosed more generally, for clarity and consistency, the IESBA developed extant paragraph R114.1 into three separate paragraphs – revised paragraph R114.1, and new paragraphs R114.2 and R114.3:

- Revised paragraph R114.1 sets out the circumstances in which a PA should comply with the principle of confidentiality.

  It contains extant paragraph R114.1 bullets (a), (b), (c), and (g). A refinement was made in bullet (d) (i.e., extant paragraph R114.1 bullet (g)) to emphasize a PA's obligation to comply

with the duty of confidentiality as set out in the Code. This refinement mirrors the PA's obligation in the lead-in of the paragraph.

- New paragraph R114.2 sets out the circumstances in which a PA cannot use or disclose confidential information, including the prohibitions contained in extant paragraph R114.1 bullets (d), (e), and (f).

  Additionally, the new paragraph has strengthened the principle of confidentiality in:

  - Bullet R114.2(a) (i.e., extant paragraph R114.1 bullet (d)), by withdrawing the extant text "outside the firm or employing organization" so as to extend the prohibition on disclosing confidential information to include other individuals within a PA's own firm or employing organization.
  - Bullet R114.2(b) (i.e., extant paragraph R114.1 bullet (e)), by making it explicit that the provision applies insofar as it concerns using confidential information for the advantage of the firm or employing organization, or the PA or a third party. Furthermore, the revised provision clarifies that confidential information acquired in the course of professional and business relationships must not be used for any advantage, whether personal or not. This avoids the situation where a PA has to determine what is considered an advantage (directly or indirectly) of a personal nature.
  - New bullet R114.2(d) was added to emphasize that a PA's duty of confidentiality as set out in the Code applies even if information, which was confidential when acquired in the course of a professional or business relationship, subsequently becomes publicly available (whether lawfully or unlawfully). See also paragraphs 37 and 38 below.

- New paragraph R114.3 provides an exception to paragraph R114.2 by detailing the specific conditions under which it is possible to use or disclose such information: *"(a) there is a legal or professional duty or right to do so; or (b) this is authorized by the client or any person with the authority to permit disclosure or use of the confidential information and this is not prohibited by law or regulation."*

  In developing the specific conditions for this exception, the IESBA took into account the existing concepts in the Code contained in:

  (a) Extant paragraph 114.1 A1(b) which states that disclosure of confidential information might be appropriate when it *"is permitted by law and authorized by the client or the employing organization*;*"* and

  (b) Extant paragraph R114.1(d) which states that a *"PA shall not disclose confidential information … without proper and specific authority, unless there is a legal or professional duty or right to disclose."*

  Building on these extant concepts, the new paragraph R114.3 recognizes that laws and regulations will generally not *expressly permit* use or disclosure of confidential information for specific purposes. The provision explains what is meant by proper and specific authority. Accordingly, the specific conditions for the use or disclosure of confidential information focus on whether the specific use or disclosure of confidential information is *expressly prohibited* by law or regulation, and specify from whom the authorization to use or disclose confidential information should come. Accordingly, the related extant provisions noted in (a) and (b) above were withdrawn.

Applicability and Interaction with the NOCLAR Provisions

35. The revisions to Subsection 114 do not impact the applicability of the extant Code provisions on responding to non-compliance with laws and regulations (NOCLAR) with respect to Subsection 114. That is, PAIBs and PAPPs continue to have a right, under new paragraph R114.3, to make a disclosure of NOCLAR or suspected NOCLAR to an appropriate authority under the conditions specified in Sections 260 and 360, respectively, subject to any confidentiality restrictions in law or regulation. Under the building blocks approach of the Code, the IESBA affirmed that no additional reference to NOCLAR within Subsection 114 is necessary.

36. Conforming amendments to the NOCLAR provisions in Parts 2 and 3 of the Code were made to update relevant paragraph references arising from the new paragraphs R114.2 and R114.3.

Duty of Confidentiality As Set Out in the Code Relating to R114.2(d)

37. New bullet R114.2(d) addresses a PA's obligation to comply with the principle of confidentiality where information acquired in the course of professional and business relationships has become publicly available, whether properly or improperly.

38. In developing this new bullet, the IESBA considered:

- Whether information that has become properly available publicly still meets the definition of "confidential information" in the Glossary.

  In this regard, the IESBA noted that the bullet refers to "information" and not "confidential information," recognizing that once it is publicly available, the information no longer meets the definition of confidential information in the Glossary. Nevertheless, the IESBA reaffirmed that despite such information becoming publicly available, a PA still needs to comply with the principle of confidentiality as the PA has acquired such information in the course of professional and business relationships, unless the conditions for exception set out in new paragraph R114.3[9] are met. The following paragraph further details the IESBA's rationale.

- Whether the phrase "…publicly available, whether properly or improperly" would appear to encompass more scenarios than necessary, as it might mean that a PA will need to seek authorization to use or disclose information, either at the outset of the professional activity or prior to use or disclosure, where that information has already been made publicly available by a client, for example in relation to time-restricted market-sensitive information subsequent to the information being made public.

  The IESBA reaffirmed that a PA continues to have an obligation to comply with the principle of confidentiality in relation to any information acquired in the course of professional and business relationships.

  Accordingly, a PA's duty of confidentiality as set out in the Code begins when such information is acquired and continues until permission to disclose or use such information is given by the client or other appropriate authority. The rationale for this approach is to avoid a PA:

[9] As an exception to paragraph R114.2, a professional accountant may disclose or use confidential information where:

(a) There is a legal or professional duty or right to do so; or

(b) This is authorized by the client or any person with the authority to permit disclosure or use of the confidential information and this is not prohibited by law or regulation.

  - Inadvertently disclosing more information than is publicly available (e.g., sharing certain additional nuances about the information upon disclosure), and preventing a subsequent chain of disclosures by the recipient(s) of such information to other unknown recipient(s).
  - Trying to determine whether disclosure occurred properly or improperly, which would require both knowledge of how the disclosure occurred, as well as any applicable jurisdiction-specific legal considerations.

- How the bullet interacts with new paragraph 114.1 A1 on taking appropriate actions to protect the confidentiality of information acquired in the course of professional and business relationships; and specifically, what might be considered the appropriate level of action to protect information which is already publicly available.

  The IESBA considers that it will be a matter of exercising professional judgment depending on the specific facts and circumstances, notwithstanding that a PA must continue to comply with the principle of confidentiality, unless they have an exemption under the conditions set out in paragraph R114.3.

  For example, a PA might be undertaking an engagement in relation to a potential transaction such as the delisting of shares in a listed entity or an acquisition by a listed entity. News about such potential transaction might become publicly available through no breach on the part of the PA. In such circumstances, regardless of how the information becomes publicly available, the Code guides the PA ~~continue~~ to take appropriate action to protect the confidentiality of the information that has been provided to perform the engagement.

Use or Disclosure of Confidential Information – Paragraph 114.3 A3

39. New paragraph 114.3 A3 has been developed to provide examples of circumstances where a PA might seek authorization to use or disclose confidential information.

40. In this regard, the IESBA recognized that at times the authorization obtained by a PA could be of a general nature. This is currently observed in some contracts signed between firms and their clients. These contracts contain general clauses that permit the use of confidential information acquired in the course of a professional activity for the purposes of the firm's internal training or other quality enhancement initiatives. Accordingly, this example has been made explicit in the paragraph, with the reference to "internal training" intended to encompass the training of both internal AI systems and staff in either a firm or an employing organization.

41. With respect to the specific circumstances where a PA seeks and obtains authorization to use or disclose confidential information, the paragraph:

    - Sets out what a PA might communicate when seeking the authorization, preferably in writing.
    - Specifies that such authorization should be sought from the individual or entity that provided the confidential information.

      This is to avoid the reader potentially misconstruing that such authorization could be obtained from the party giving instructions in relation to the proposed use of the confidential information (for example, an external training organizer, a development or research company, or an entity commissioning a benchmarking survey, etc.).

- The information that a PA might communicate to the individual or entity that provided such information includes:
    - The nature of the information to be used or disclosed.
    - The purpose for which the information is to be used or disclosed (for example, technology development, research or benchmarking data or studies).
    - The individual or entity who will undertake the activity for which the information is to be used or disclosed.
    - Whether the identity of the individual or entity that provided such information or any individuals or entities to which such information relates will be identifiable from the output of the activity for which the information is to be used or disclosed.

42. The IESBA acknowledges that there may be occasions when the identity of the individual or entity will be apparent from the raw data – for example, in the collection phase of the relevant data for the inputs for AI training or preparation of benchmarking surveys. Therefore, as a practical and critical consideration, the last bullet focuses on the need to consider whether the identity of the individual or entity that provided such information or any individuals or entities to which such information relates will be identifiable from the output of the activity for which the information is to be used or disclosed.

43. The IESBA also considered whether it is possible to completely anonymize data when using it, or at least for the purpose for which the information is to be used (i.e., the output). The IESBA noted that there are indeed many tools and techniques to perform such complete anonymization, notwithstanding also the availability of various tools and techniques which enable the anonymization to be reversed. Such risks will have to be assessed and balanced by a PA when determining whether they should go ahead with anonymizing confidential information.

Other Matters

44. Responsive to other principal points and suggestions raised by ED respondents, the IESBA has:

- Replaced the term “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.
- Replaced the term “public domain” in the Glossary definition of confidential information with “is not publicly available” to avoid association with intellectual property rights.
- Added a consideration of *“any applicable law or regulation (including those governing privacy) in a jurisdiction where disclosure might take place and where the confidential information originates”* to revised paragraph 114.3 A2. This addresses a suggestion from respondents to highlight the consideration of privacy, cross-border scenarios, and potential conflicts with local laws and regulations. This revision supplements the overriding provisions in extant Code paragraphs R100.7 to 100.7 A1 of the Code which govern differences between the Code’s provisions and local laws and regulations.

  The IESBA also deliberated if consideration of laws and regulations addressing where information is stored (e.g., a cloud-based facility) should be incorporated into the revisions. However, the IESBA noted that paragraph 114.3 A2 is only intended to provide a list of examples of factors for a PA to consider and that it is not possible to highlight every

circumstance or permutation of law or regulation that might be applicable.

C. Complex Circumstances (Section 120)

Technology ED

45. The ED 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. In developing the proposals, the IESBA considered:

- The concepts explained in the August 2021 thought leadership paper *Complexity and the Professional Accountant: Practical Guidance for Ethical Decision-making*, to which the Technology Working Group contributed. In particular, the paper explained:

> *"Complicated problems can have many causes that are interacting, but they can be broken down and addressed piece-by-piece. Outputs are predictable and proportionate to inputs and the resulting problems are solvable, and once solved, the formula, algorithm, tool or approach can be readily applied the next time with predictable consequences.*
>
> *Complex problems and systems, in contrast, include factors that are…both dynamic and interactive in ways that are difficult or impossible to predict. … Small changes in inputs can have a disproportionately large impact on outputs, and interactions between elements can lead to unexpected synergies.*
>
> *Because of the ambiguity and lack of explainability [over cause and effect], the rules, processes and algorithms that might be effectively applied to complicated problems fall short for complex circumstances, [and the complex circumstance must instead be managed holistically]."*

- Stakeholder feedback from the October 2020 survey *Technology and Complexity in the Professional Environment* noted general support from respondents for more guidance in the Code to help PAs navigate complex circumstances. In particular, 82% of respondents supported highlighting complexity as a pervasive factor in decision-making while applying the conceptual framework.[10]

46. Taking into account these considerations, the ED proposals reflected the IESBA's view that:

- The terms "complex" and "complicated" are often used interchangeably by the general public, including the average PA. Therefore, it is anticipated that PAs might turn to the new application material on complex circumstances whenever they encounter unclear, difficult, complicated or complex circumstances. In this regard, there would not be a downside to a PA considering the factors to manage complex circumstances in addition to applying the conceptual framework.
- Although complex circumstances have always existed and are not a new phenomenon specific to technology, rapid digitalization has increased the interconnectedness of social, economic, legal and geopolitical systems, and is a complex circumstance that PAs are now facing. In this

[10] The survey detailed four options to incorporate the notion of "complexity" in the Code. Stakeholders were able to select one or more options as their preferred route to addressing "complexity" in the Code. The option to incorporate complexity as a factor in applying the conceptual framework had the highest number of stakeholders selecting it.

regard, the guidance should not be restricted to technology-specific complex circumstances.

Feedback from ED Respondents

47. Support was mixed for these proposals. While some respondents supported the proposals, others did not support them or expressed reservations. In this regard, the following substantive comments were made:

- In considering whether it is necessary to include such guidance 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. In both cases, the PA is required to attain and maintain the professional knowledge and skills necessary to provide a competent professional service.
  - The identification and management of complexity would not change the consideration of threats and safeguards in the Code, or the requirement for a PA to consider new information or changes in facts and circumstances.
- The notion of complexity could be instead incorporated into a factor to be considered when evaluating threats to compliance with the fundamental principles, or into application material for considering changes in facts and circumstances, both of which are part of the application of the conceptual framework.
- The concept of “complexity” in the Code should be aligned with how it is considered in ISA 315 (Revised),[11] which includes “complexity” as one of the "inherent risk factors." Doing so would encourage a greater degree of convergence between the approaches in the Code and the ISAs.
- “Complexity” may, to some degree, always exist because it is a relative term that is open to interpretation depending on the individual’s background, skills, and experience. The guidance should therefore reflect a level of scalability in that there might be circumstances that are not “complex” even if they involve both elements that are uncertain, and multiple variables and assumptions.
- The proposal is vague, general and not technology-specific, and if the proposal is finalized as drafted, non-authoritative material should be developed to explain how the guidance should be applied in practice.
- Technology-specific examples of complex matters should be illustrated in the Code.

IESBA Decisions

48. On balance, given the qualified support for the provisions (in addition to the support from the October 2020 survey to highlight complexity as a factor when applying the conceptual framework), the IESBA considered that there is a benefit in retaining some form of guidance on complexity.

49. To address the concerns raised by respondents, the IESBA made revisions to the ED to incorporate

[11] International Standard on Auditing (ISA) 315 (Revised), *Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and Its Environment*

the notion of complexity as part of exercising professional judgment when applying the conceptual framework in new paragraphs 120.5 A6 to A8. Specifically, the revisions build on material contained in extant paragraphs 120.5 A4 and A5. The revisions highlight that complexity is a factor to consider when exercising professional judgment, rather than a discrete circumstance that increases the challenges of applying the conceptual framework.

50. This approach recognizes that the circumstances in which PAs carry out professional activities and the factors involved vary considerably in their range and complexity. It is therefore, conceptually aligned with the concept of complexity in ISA 315 (Revised), which will promote consistent application between the ISAs and the Code.

51. In new paragraph 120.5 A6, drafting enhancements were also made to the description of complexity so that it is easier for PAs to understand and apply (i.e., *"…the compounding effect of the interaction between, and changes in, elements of the facts and circumstances that are uncertain, and variables and assumptions that are interconnected or interdependent..."*), while taking care to retain the substance of the ED proposals and thought leadership that informed it.

52. The application material on managing complexity is fundamentally unchanged apart from:

- The addition of a new factor in new paragraph 120.5 A8 *"analyzing, and investigating, as relevant, any uncertain elements, the variables and assumptions and how they are connected or interdependent*," based on respondents' suggestions.
- Emphasizing that the concepts of "being alert" and "communicating inherent uncertainties or difficulties" in new paragraph 120.5 A7 are already requirements in the Code by cross-referencing to the extant paragraphs, responsive to input from a MG member.

53. Finally, the IESBA considered whether it is appropriate to include technology-specific examples into the Code, but concluded that it would be too detailed to do so for a principles-based Code, and more appropriate for non-authoritative material, such as the thought leadership paper already issued. Accordingly, the IESBA reaffirmed its position not to restrict the guidance to a specific technology example, given that the application material is applicable to all circumstances. For the reasons set out in paragraph 46, the IESBA also reaffirmed that there would be no downside to applying the approach in new paragraphs 120.5 A6 to A8 in the course of a PA's performance of a professional activity.

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

Technology ED

54. The ED proposals introduced:

(a) Examples of matters to be considered when identifying threats that might be created when PAs rely upon the output from technology; and

(b) 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.

Feedback from Respondents

55. Respondents were generally supportive of the proposals and provided suggestions for additional factors and enhancements to drafting.

56. With respect to the considerations on identifying threats, the principal points and comments raised were as follows:

- The matters identified should be linked to specific threats to compliance with the fundamental principles and a sub-heading should be added.
- 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. Recommendation B of the Technology Working Group's Phase 2 Report also highlights this issue.
- It was not clear how the penultimate ED bullet "whether technology incorporates expertise or judgements of the accountant or the employing organization/firm" creates a self-interest threat or self-review threat, whether the expertise or judgment being referred to relates to that of the PA (i.e., exercising professional judgement) or relates to the use of the technology (i.e., setting parameters of technology), and whether there is a need to distinguish between technology developed in-house or licensed externally.
- Various 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., the sufficiency of data quality and programming underpinning the technology).
    - The level of sophistication or maturity of the technology as that will impact the availability of information about how the technology functions or how widespread (i.e., commonly accepted) the technology is.
    - Specific issues to be considered by PAs in relation to the training of AI systems.
- Safeguards to address 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.

57. With respect to the considerations for determining whether reliance on or use of the output of technology is reasonable or appropriate for the intended purpose, the principal points and comments raised were as follows:

- 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 judgments 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.
- The guidance should emphasize the whole process of making use of a technological resource, rather than the use of the output of the technology.
- Suggestions for additional factors to be included, 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.
  - Whether an organization's general and application controls related to the technology are effective.
  - Emphasizing the accountability of PAs – which is particularly relevant where the decision-making is automated – by adding a consideration of the "decisions made by individuals relating to the operation of the technology."

- To further clarify:
  - How the ED bullet relating to the reputation of a software developer should be assessed (i.e., reputation could be subjective and unreliable without further due diligence) and how this factor might impact the PA's consideration when it is not possible to assess the developer's reputation, especially where emerging technology is involved.
  - That a firm's or employing organization's oversight of technology will be different depending on whether the technology is developed in-house or purchased from third parties.

    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. In this situation, the emphasis should be on assessing the vendors and whether they have provided sufficient information for PAs to have oversight of the third-party technology.

IESBA Decisions

58. The revisions to the ED in Parts 2 and 3 of the Code address most of the principal points and suggestions raised.

Sections 200 and 300

59. In relation to the examples of facts and circumstances that might create a self-interest threat in paragraphs 200.6 A2 and 300.6 A2, the IESBA:

- Considered respondents' feedback that it is not immediately clear why and how some of the examples create a self-interest threat. The IESBA noted that the examples are based on the requirement to act with sufficient expertise as set out in Section 230. In particular, paragraph 230.2 states that "acting without sufficient expertise creates a self-interest threat to compliance with the principle of professional competence and due care," and paragraph 230.3 A2 sets out examples of facts and circumstances regarding what constitutes acting without sufficient expertise from the broader perspective of a PA performing their professional activities. Such examples are conceptually aligned with those set out in paragraphs 200.6 A2 and 300.6 A2.

  Accordingly, the IESBA determined to add a reference to Section 230 *Acting with Sufficient Expertise* under the relevant examples in paragraphs 200.6 A2 and 300.6 A2 so that readers can better understand why and how a self-interest threat is created.

- Reworded the examples to reflect a PA's accountability to make ethical decisions when they encounter situations where the data is insufficient or the technology is inappropriate.

The ethical challenge is whether the PA will act in their own self-interest (for example, so that they can meet deadlines or earn a fee) and continue to use such insufficient data or inappropriate technology when undertaking a professional activity. This is reflected in the examples with the addition of the phrase "might not." The IESBA noted that this phrase is necessary because otherwise the PA would automatically fall into a breach of the fundamental principle of professional competence and due care.

60. The IESBA noted that the examples of "safeguards" provided by respondents are akin to considering the existence of conditions, policies and procedures to evaluate the level of a threat, rather than true safeguards as defined in the Code. As such, new paragraphs 200.7 A4 and 300.7 A6 were developed to provide examples of circumstances 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 or firm and its operating environment.

61. 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 IESBA 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 IESBA agreed that there is benefit to developing guidance in this area and noted that the Technology Working Group's Phase 2 Report highlights considerations for PAs in relation to the use or development of AI systems.

62. The IESBA 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 IESBA concluded that it would be impossible to do so since each situation would depend on the specific facts and circumstances.

Sections 220 and 320

63. As regards the concerns relating to the focus on the "output of the technology," the IESBA reaffirmed its decision to use that phrase as the "output of the technology" is ultimately what a PA will utilize in the delivery of their professional activity or service. However, in order to be able to use such output, the whole process of making use of the technology is considered within the application material, which can be seen from the following factors included in paragraphs 220.8 A1 and 320.11 A1:

- 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, …, and decisions made by individuals in the course of using the technology.

64. Concerning how a firm or employing organization exercises "oversight" for in-house versus third-party technology, the IESBA is of the view that such oversight will indeed differ depending on the facts and circumstances and that such differences in approach do not only arise in relation to the use of technology.

Using the Work of Others/Experts

65. Finally, the IESBA also aligned the drafting approach of paragraph 320.10 A1 with extant paragraph

220.7 A1. Such alignment recognizes that the use of an expert in Part 3 involves consideration of "whether the expert is subject to applicable professional and ethics standards," rather than the extant presumption that the expert has applicable professional and ethics standards. In this regard, the IESBA approved a project on the "Use of Experts" in December 2022 to develop enhancements to the Code addressing:

- Ethics and independence considerations relating to the use of an external expert in audit and assurance engagements.
- Ethics considerations regarding the involvement of an expert (both internal or external to the employing organization or firm) in the preparation and presentation of financial and non-financial information, including sustainability information, and other activities.
- Ethics considerations regarding the involvement of an expert (both internal or external to the employing organization or firm) in the provision of other services (such as tax planning and technology-related activities).

E. Close Business Relationships (Section 520, Conforming Amendments in Section 920)

Technology ED

66. The ED included a signpost in Section 520 *Business Relationships,* to prompt firms to consider the relevance of the NAS provisions in Section 600 when technology is provided, sold, resold or licensed by a firm or network firm to an audit client. This reflected the IESBA's view that:

    - Such a prompt is necessary to address the fact that a significant minority – 24% of respondents to the October 2020 survey The Impact of Technology on Auditor Independence – did not think that the NAS provisions were relevant when a firm sells or licenses technology that performs a NAS. The signpost was intended to guide users of the Code who look to Section 520 in such circumstances to appropriately consider the provisions in Section 600.
    - 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 or associated services provided by the firm or a network firm. In either case, firms are prompted to consider whether the NAS provisions (i.e., Section 600) are relevant to the facts and circumstances of the reselling arrangement.

67. The ED also added an example of a technology-related close business relationship and included the concepts of "selling" and "reselling" to the existing examples of close business relationships where a firm or a network firm distributes or markets a client's products or services, or vice versa. In finalizing the ED, the IESBA discussed including another example of a close business relationship related to software licensing arrangements between a firm and its client, and factors that might impact the closeness of such business relationship. The ED proposals reflected the IESBA's view not to include such an example because it would require an elaboration of the nature of the specific sale or licensing arrangement in order for readers to understand the nature of the firm's interests in that arrangement, and doing so would detract from the principles-based nature of the Code.

Feedback from Respondents

68. Respondents were mainly supportive of the proposed signpost in the ED, although a few respondents did not support it or expressed reservations. In particular, concerns were raised that:

- The reference to Section 600 within Section 520 might confuse users of the Code since the independence considerations for NAS and close business relationships are different.
- The application material gives the impression that pure reselling or selling is a non-assurance service, although this is not always the case. For example, in relation to the resale of third-party technology in "pure pass-through" situations, Section 600 may not be relevant.

69. It was also suggested that additional clarity on the "indirect" provision of services be provided, i.e., where firms have developed software for non-audit clients, who subsequently use this software to provide a service to those firms' audit clients.

70. There was general support for the example of a close business relationship arising from the provision of technology. Suggestions were provided to include other examples, such as 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.

71. There were also suggestions to include a general principle for the identification or assessment of "close business relationships" and a definition of "business relationship," recognizing that the examples provided cannot cover all scenarios.

IESBA Decisions

Consideration of the Relevance of the NAS Provisions

72. The IESBA reaffirmed that it is necessary to include the signpost (i.e., reference to the NAS provisions) as set out in paragraph 520.7 A1, given the survey results that were the impetus for its inclusion. However, to avoid giving the impression that pure reselling immediately equates to providing a NAS, the IESBA has revised the wording of the signpost to emphasize that the provisions in Section 600 would apply if they are relevant to the specific facts and circumstances. Specifically, the IESBA acknowledges that pure reselling, i.e., "pass-through" reselling arrangements which have no other services (including any ancillary or associated services) combined or attached, does not constitute a NAS.

73. In addition, the signpost has been expanded to prompt the PA to assess if "indirect" services are being provided. For example, Section 600 would be relevant where firms have developed software for non-audit clients who use such software to provide services that constitute a NAS for its end users (i.e., the non-audit client's own customers) and where such end users are also audit clients of the firm. In developing this guidance, the IESBA debated whether, in all instances, a firm will know if the end customer is an audit client of the firm. In this regard, the IESBA noted that firms might address this uncertainty by considering whether it is appropriate to establish policies and procedures which can facilitate the identification and monitoring of such situations.

Close Business Relationships

74. New application material in paragraph 520.3 A3 addresses, at a principles-based level, respondents' suggestion to add other examples of close business relationships. In light of the varied nature of these licensing arrangements and how the technology is used, the IESBA explicitly emphasized that such arrangements *"might create"* a close business relationship and that it *"depends on the specific facts and circumstances."* For example, the IESBA observed that there are a number of instances where such arrangements are purchases in the ordinary course of business (i.e., a firm licensing from

an audit client products or solutions which comprise office software), and as such, do not normally create a threat to independence.

75. The IESBA's view is that the approach taken will prompt users of the Code to consider, in general, whether the products or solutions being licensed give rise to a close business relationship, recognizing that it is impossible to list all the circumstances of technology-related close business relationships. The use of the term "solutions" in paragraphs 520.3 A2 and 520.3 A3 is intended to refer to those solutions related to technology, for example, solutions which might be "software as a service."

76. With respect to the suggestions to add a general principle for identifying or assessing close business relationships or adding a definition of business relationships, the IESBA noted that this is outside the scope of the technology project, but that such feedback can inform a potential future workstream to comprehensively review Section 520, a topic which is being considered in the IESBA's 2024-2027 strategic work plan consultation paper.

Buying of Goods and Services

77. The IESBA determined to make a refinement to paragraph 520.6 A1 to recognize that the licensing of technology in the normal course of business and at arm's length does not usually create a threat to independence. This clarification was made as such licensing is fairly common in today's digitally enabled world. It also serves as an example of when an arrangement under which the firm or a network firm licenses products or solutions *from* a client (i.e., paragraph 520.3 A3) does not usually create a close business relationship. See also the discussion on close business relationships above.

78. The phrase "purchase of goods and services" encompasses those purchased through digital platforms.

F. Hosting (Subsection 606, Conforming Amendments in Section 900)

Technology ED

79. The ED set out examples of assuming management responsibility in relation to IT systems services, and these services would therefore be prohibited for all audit clients (ED paragraph 606.3 A1). The proposal further expanded on the prohibition on assuming management responsibility in extant paragraphs R400.15 and revised paragraph R606.3.

80. The ED position reflected the IESBA's view that if a firm or network firm provides IT systems services such as:

    (a) Hosting of an audit client's data as a service (either directly on internal servers or indirectly on a cloud provider's server); and

    (b) Operating an audit client's network security, business continuity or disaster recovery function,

    a firm would not be able to meet the precondition that the audit client's management will make all the judgments and decisions that are the proper responsibility of management, as set out in paragraphs R400.16 and R606.3.

81. However, the proposal acknowledged that a firm or a network firm collecting, receiving and retaining audit client data to enable the provision of a permissible service does not result in the assumption of a management responsibility.

Feedback from ED Respondents

82. Respondents generally supported the proposal, although a few respondents did not support it or expressed reservations. The principal concerns related to the potentially unclear interpretation of the prohibition. In particular:

- Whether the phrase "provides services in relation to hosting" includes, for example, 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.
- Whether the scope of the prohibition was 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. 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.
  - The hosting of any data irrespective of whether it is the client's source or primary data, or a copy of it.
- Suggestions were made that the examples should give consideration to the type of data being hosted, the method of hosting, and the purpose of the hosting.
- Suggestions were also made that the phrase "directly or indirectly" should be expanded upon in the Code.

IESBA Decisions

83. Revisions were made to the ED paragraph 606.3 A1 to address the comments raised by respondents. In particular, the IESBA determined to:

- Replace the phrase "services in relation to hosting" in the ED lead-in with "stores data or manages" to be more specific as to the type of hosting services covered by the prohibition.
- Add three new sub-bullets to provide examples of when a specific method or purpose of hosting would involve an assumption of management responsibility.

84. The IESBA's view is that further explanation of the phrase "directly or indirectly" is not necessary in the Code as the premise for including it is to ensure that all and any means of storing data or managing the hosting of data is covered by the prohibition. Therefore, it does not matter if the activity is conducted directly on internal servers or indirectly on a cloud provider's server.

85. New paragraph 606.3 A2 acknowledges that the collection, receipt, transmission and retention of data provided by an audit client in the course of an audit or to enable the provision of a permissible service to that client does not result in an assumption of management responsibility. The IESBA determined to add the term "transmission" to this provision to highlight that portals for transferring information in the course of providing a permissible service are not prohibited. The IESBA also added the term "in the course of an audit" to clarify that transmission of information in such circumstances is not precluded. Therefore, in accordance with paragraph 606.3 A2, retention of data provided by an audit client (e.g., for quality control purposes, statutory inspection purposes, etc.) does not constitute assuming a management responsibility while the audit or service is ongoing or when it has been completed.

86. Finally, the IESBA also deliberated whether the conforming amendments in paragraphs 900.13 A4 and A5 of the revisions might be better placed in Section 950, which addresses NAS. However, since the material is specific to examples of IT systems services *that result in the assumption of a management responsibility,* the IESBA views that it is appropriately positioned under the overarching requirements and application material relating to the prohibition on assuming management responsibility. Relocating such material to Section 950 would have the consequence of creating a need to develop revisions to further expand on what constitutes management responsibility and provide other examples (in particular, since Section 950 is not specific to IT systems services, compared to Section 606).

IV. Other Comments Related to Revisions to the ED

90. Other revisions arising from the IESBA's review and analysis of the comment letters included those in the following areas:

- Transparency.
- Ethical Leadership.
- General Non-assurance Services Provisions.
- "Routine or Mechanical" and Management Responsibility.
- IT Systems Services and Self-review Threat.
- Non-financial Reporting and Self-review Threat.

Transparency

91. The ED proposal expanded the extant Code requirement for PAs to be transparent with their employing organization, firm, or any relevant stakeholder about the limitations inherent in the services and activities that the PA provides (paragraph R113.3). Specifically, it strengthened the requirement for a PA to provide such stakeholders with "sufficient information to understand the implications of those limitations."

92. Responsive to respondents who questioned what sufficient information would consist of, and who is in a position to judge its sufficiency, the IESBA has refined the drafting to read *"explain the implications of those limitations"* so that the threshold of what the PA has to achieve with such communications is explicitly set out.

Ethical Leadership

93. The ED proposal expanded on the extant application material which highlights the expectation that a PA will encourage and promote an ethics-based culture in their organization, taking into account their position and seniority. Specifically, it included the expectation that a PA "demonstrate ethical behavior in dealings with business organizations and individuals with which the accountant, the firm or the employing organization has a professional or business relationship."

94. The IESBA made revisions to address respondents' key comments and suggestions to:

- Clarify whether the term "demonstrate" implies additional documentation, or whether it means that a PA's behavior needs to be obvious. In this regard, the IESBA replaced the term "demonstrate" with "exhibit" to clarify that it is to do with the PA's behavior.

- Consider PAs' interaction with public sector organizations as the term "business organizations" seemed to exclude such organizations. The IESBA determined to replace that term with "entities" to broaden the intended scope.
- Update extant paragraph 200.5 A3 to reflect the broadened expectations of ethical leadership.

95. Finally, the IESBA added new paragraph 300.5 A2 in response to suggestions that the extant paragraph 200.5 A3, as revised for the technology project, should be mirrored in Part 3 of the Code.

General Non-assurance Services Provisions

96. The ED proposals added upfront introductory material in Section 600 to make clear that the NAS provisions apply when a firm or a network firm uses technology to provide a NAS to an audit client (ED paragraph 600.6). The ED reflected the IESBA's position that such guidance encompasses:

- All the possible ways in which a firm or a network firm might perform a NAS, including, for example, when a firm or network firm uses technology (whether from a third-party or developed internally) to perform a NAS for an audit client.
- Where a firm or a network firm provides, sells, resells or licenses technology to an audit client.

97. Responsive to respondents' comments, the IESBA added a consideration of "indirect" services provided to an audit client (paragraph 600.6(b)).

"Routine or Mechanical" and Management Responsibility

98. The ED proposals included new application material to remind PAs that automated accounting and bookkeeping services are not necessarily "routine or mechanical" (ED paragraph 601.5 A2). The proposal elaborated on the IESBA's position that "routine or mechanical" accounting and bookkeeping services: (a) involve information, data or material in relation to which the client has made any judgments or decisions that might be necessary; and (b) require little or no professional judgement (extant paragraph 601.5 A1).

99. The ED proposal also introduced new application material under the general requirements and application material relating to the prohibition on the assumption of management responsibility in Section 400. This material further emphasized that regardless of whether technology is used in performing a professional activity for an audit client, the prohibition on assuming a management responsibility applies (ED paragraph 400.16 A1).

100. The IESBA made revisions taking into account various drafting enhancements suggested by respondents. The principal comments raised are as follows:

- Whether the term "mechanical" in the phrase "routine or mechanical" continues to be appropriate since it overlaps with the term "automated" in paragraph ED 601.5 A2.

  The IESBA acknowledges the overlap but determined to make no change given that "routine or mechanical" is a long-standing phrase that has been widely used and understood. Furthermore, the revised NAS provisions effective in December 2022 introduced paragraph 601.5 A1 to expand on what is "routine or mechanical." Deleting the term "mechanical" without any intention of changing the outcome of applying such a phrase might cause confusion to users of the Code.

- Whether the application material in ED paragraph 400.16 A1 was necessary, and whether such

material is overly broad – i.e., it would appear to cover technology such as email.

The IESBA reaffirmed that such material is necessary to address a view that emerged from the NAS project that automated services might not involve an assumption of management responsibility. In this regard, the purpose of the material is to make it clear that whenever technology is used – whether to supplement a PA's activities or in place of a PA – the possibility of an assumption of management responsibility might arise. The IESBA further reaffirmed that the revisions apply to all forms of technology, ranging from email to AI.

101. The factors to be considered in determining whether an automated service is routine or mechanical include, among others, whether the automated service relies on technology that is based on or requires the expertise or judgment of the firm or network firm. Such expertise or judgment includes the methodology of the technology (such as the logic of the algorithm) because it might affect, for example, the reliability of inputs, the assumptions or parameters used, or the interpretation of outcomes. The determination of whether the accounting and bookkeeping service meets the criteria of "routine or mechanical" is important because such services are permissible for audit clients that are not public interest entities (PIEs). Otherwise, such services are prohibited.

IT Systems Services and Self-review Threat

102. The ED proposed to modernize and strengthen the independence requirements for IT Systems Services. Apart from the proposals in relation to examples of services that result in a management responsibility discussed in Section III, it proposed to:

- Expand the description of IT systems services to highlight the fact that services related to IT systems can extend beyond the design, development and implementation of hardware or software systems.
- Provide additional examples of IT systems services that might create a self-review threat and are therefore prohibited for PIE audit clients.
- Withdraw the extant approach for the provision of services involving the implementation of certain "off-the-shelf" accounting or financial reporting software to recognize that such software in today's digital world is likely to be licensed directly from the software provider and is typically tailored as part of the implementation process.

103. The IESBA made refinements taking into account respondents' suggestions. In addition, the revisions give explicit consideration to cyber-security, which is increasingly relevant in today's world, and addressed respondents' suggestions. Specifically, the example of a self-review threat in terms of "designing, developing, implementing, operating, maintaining, monitoring or updating IT systems" has been expanded to include those related to cybersecurity.

104. The IESBA was careful to balance the public interest elements of providing such services to small- and medium-sized entities (SMEs) versus prohibiting such services due to the creation of the self-review threat. Therefore, for non-PIE audit clients, such services are permissible, provided that the firm applies the conceptual framework to the particular facts and circumstances. For PIE audit clients, the services addressed in paragraphs 606.4. A1 to A3 are prohibited when they form part of or affect an audit client's accounting records or system of internal control over financial reporting.

105. Finally, the IESBA is cognizant that there are some cybersecurity services that might be requested by clients that – depending on the facts and circumstances – might be akin to the provision of advice

and recommendations. In this regard, the IESBA reaffirmed that the revisions in Subsection 606 would not immediately preclude firms from providing advice and recommendations in relation to IT systems, including cybersecurity, to their audit clients. However, firms would need to apply the extant general provisions relating to the provision of advice and recommendations in paragraphs 600.11 A1, R600.14, and R600.16 to 600.17 A1.

Non-financial Reporting and Self-review Threat

106. The ED proposals preserved the existing alignment between Parts 4A and 4B of the Code. The ED proposals:

- Added an explicit statement in revised paragraph 900.1 to indicate that Part 4B of the Code applies to assurance engagements relating to an entity's non-financial information, for example, environmental, social and governance (ESG) disclosures.
- Added an example to explain that the provision of certain types of IT systems services might create a self-review threat in relation to the subject matter information of an assurance engagement, i.e., *"designing, developing, implementing, operating, maintaining, monitoring, updating IT systems or IT controls and subsequently undertaking an assurance engagement on a statement or report prepared about the IT systems or IT controls."*

107. Regarding certain types of IT systems services that might create a self-review threat, the IESBA made revisions to include an additional example to the ED proposal. As suggested by respondents, this example explicitly considers the following: *"designing, developing, implementing, operating, maintaining, monitoring, updating or upgrading IT systems and subsequently issuing an assurance report on subject matter information, such as elements of non-financial information, that is prepared from information generated by such IT systems."* The IESBA believes this additional example to be particularly relevant given the exponential rise in services pertaining to sustainability. In this regard, the IESBA approved a project in December 2022 to develop ethics and independence for sustainability reporting and assurance.

V. Other Matters

108. Other substantive matters raised by respondents and considered by the IESBA are set out below.

Documentation Expectations

109. Respondents questioned what the expectations are for documentation by the PA in relation to the revisions pertaining to Parts 1 to 3 of the Code.

110. The IESBA considered whether further documentation considerations should be included in the revisions but determined that the current provisions related to these matters in the extant Code are sufficient. For example, this includes the documentation expectations set out in Sections 220 *Preparation and Presentation of Information,* 270 *Pressure to Breach the Fundamental Principles,* 310 *Conflicts of Interest*, 260 and 360 *NOCLAR*, as well as those set out in Parts 4A and 4B of the Code. For auditors, this is also further supplemented by the requirements in the relevant auditing standards.

111. In this regard, the IESBA noted that the need for documentation is not a consideration that arises only in relation to the use of technology. The IESBA considered that such feedback can inform a potential future workstream to holistically review the documentation provisions in the Code.

Applicability of the Revisions to Multidisciplinary Teams

112. Respondents questioned how PAs might apply the revisions in Parts 1 to 2 of the Code since PAs often work closely with others within their employing organizations or firms (i.e., IT teams) on matters relating to the use of technology and data governance, including maintaining confidentiality.

113. To this end, the IESBA noted that extant paragraphs R220.7 to 220.7 A1 and R320.10 to 320.10 A1 are relevant to a PA's use of the work of others or experts, for example, IT teams or IT experts within an employing organization or firm. Specifically, a PA should exercise professional judgment to determine the appropriate steps to take, if any, when using the work of others or an expert. The extant Code provides factors to guide the PA in this determination.

114. Additionally, the IESBA also observed 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. In this regard, the revisions bring into consideration the employing organization's overall approach to technology issues. Specifically:

- Paragraphs 200.7 A4 and 300.7 A6 recognize 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 or firm 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 highlight 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 220.11 A4 and 320.12 A1 recognize that a PA's position in the employing organization or firm will impact the PA's ability to obtain information in relation to the factors to consider in determining whether to use the work of others or the output of technology.

115. Finally, as noted above, the IESBA's new project on the "Use of Experts" involves a holistic review of the provisions in the Code addressing the use of experts from both the ethics and independence perspectives.

Applicability of the Revisions to All Technologies

116. Respondents questioned whether the revisions apply to all types of technology, such as email, Excel, AI, blockchain, etc.

117. In this regard, the IESBA reaffirmed that the revisions apply to all technologies. This is important as the revisions have been developed in a principles-based manner so that the Code remains relevant and fit-for-purpose as technology evolves.

118. Accordingly, the use of the term "technology" in the Code is broad and is meant to encompass all technologies (including "automated tools and techniques" as used in the auditing standards,[12] AI and machine learning, blockchain, and other future technologies not yet known).

119. PAs should therefore exercise professional judgment when determining the level of knowledge,

[12] The IESBA noted that the difference in terminology with respect to the IESBA's use of the term "technology," and the IAASB's use of the phrase "automated tools and techniques (ATT)" is appropriate, as the term "technology" is intended to be broad and encompasses ATT.

understanding, oversight, etc., that might be required to use technology. Use of common tools such as Excel does not preclude the possibility of threats to compliance with the fundamental principles, depending on facts and circumstances.

Potential Implementation Challenges for SMPs and PAs in SMEs

120. Respondents suggested that the IESBA consider implementation challenges or potential unintended consequences for SMPs and PAs working in SMEs, for example, segregation of duties concerns due to resource or cost constraints.

121. The IESBA has taken such considerations into account. Specifically, the ED was developed with input from the IFAC SMP AG as well as from the Technology Working Group's fact-finding work, which included outreach with PAIBs within SMEs. The revisions also considered input from the IFAC SMP AG to the ED.

Consideration of the Code's Pace of Change, Length and Increasing Requirements

122. Respondents commented on the Code's pace of change, length and increasing requirements. The IESBA noted that this is not a new concern, and that it carefully balances the need to be responsive to developments or matters of significant public interest as part of formulating its strategy and work plan against the need to allow jurisdictions and stakeholders sufficient time for adoption and implementation activities.

123. Nevertheless, in relation to the changes to the Code to address technology – the IESBA's technology workstreams were designed to address the challenge of responding to rapid technological transformations. Instead of changing the Code with every new technology, the IESBA's focus has been on developing principles-based revisions to the Code that apply to all technologies. The IESBA considers that such revisions will go a long way towards future-proofing the Code as advancements in technology continue.

124. The IESBA will now shift its focus to monitoring technology developments, allowing time for these revisions to be adopted and for stakeholders to undertake the necessary implementation efforts. This shift in focus is supported by the completion of the Technology Working Group's Phase 2 fact-finding work, which concluded that the key ethics and independence themes arising from technology transformations observed from 2019 to 2022 have become increasingly consistent over time. The broad insights gathered also remain relevant despite the different types of technology being assessed and evaluated.

125. Finally, to assist with the monitoring efforts, the IESBA has established a Technology Experts Group consisting of 8 individuals with practical experience in current and emerging technologies.

VI. Effective Date

126. As discussed above, some respondents to the ED were concerned about the Code's pace of change, length and increasing requirements.

IESBA Decisions

127. The IESBA determined that the effective date should be as follows:

- Revisions to Parts 1 to 3 will be effective as of December 15, 2024.

- Revisions to Part 4A will be effective for audits and reviews of financial statements for periods beginning on or after December 15, 2024.
- The conforming and consequential amendments to Part 4B in relation to assurance engagements with respect to underlying subject matters covering periods of time will be effective for periods beginning on or after December 15, 2024; otherwise, these amendments will be effective as of December 15, 2024.

Early adoption will be permitted.

128. In determining the effective date for the revisions, the IESBA has balanced (i) the public interest need for the revisions to take effect as soon as practicable given the rapid pace of change in technology, and (ii) the need for a sufficient period for awareness-raising activities, and for adoption and implementation at firm and jurisdiction levels.

129. The IESBA also considered the following:

- The objective [13] of the technology project was to respond, in a timely manner, to the transformative effects of major trends and developments in technology in relation to the accounting, assurance and finance functions. The public interest is served by these technology-related revisions because they will help ensure that the Code's provisions remain relevant and fit-for-purpose.
- The technology-related revisions build off the Role and Mindset and NAS revisions, which already introduced technology-related provisions into the Code. As such, most of the revisions develop the principles which are already in the Code and effective, for example, with respect to NAS, the self-review threat prohibition for PIE audit clients.
- Feedback from NSS that there should be a reasonable timeframe to allow for translation, jurisdiction-specific due processes for adoption, and the development of appropriate implementation tools and resources.[14]

[13] Project Proposal as approved in March 2020: https://www.ifac.org/system/files/meetings/files/Agenda-Item-8-Technology-Approved-Project-Proposal.pdf.

[14] In this regard, it was noted that introducing a prohibition on hosting services (in particular) with effectively an implementation period of less than a year could cause practical issues. For example, firms in the course of providing a specific NAS would face the challenge of terminating the provision of such services, with the consequential disruption and associated practical issues for the client.

Published by: IFAC International Federation of Accountants®

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