This paper reflects the Task Force’s thinking and responses to date; as informed by the IESBA’s September 2022 deliberations and advance comments on the October revised text, as well as stakeholder feedback arising from targeted stakeholder outreaches held in Q4 2022.

Subject to the IESBA’s approval of the final technology-related revisions to the Code at its November/December 2022 meeting, this paper will be updated to reflect the final IESBA Decisions accordingly.

Contents

I. Introduction ............................................................................................................... 2
   A. About the Technology-related Revisions .............................................................. 2

II. Background ............................................................................................................... 2
   A. Development of the Project Proposal and Technology-related Revisions .......... 2
   B. Objective of the Project ....................................................................................... 3
   C. Interaction with Other IESBA Work Streams and Coordination with IAASB ... 3
   D. Technology Exposure Draft ............................................................................... 4

III. Significant Matters ................................................................................................ 4
   A. Professional Skills (Section 113) ....................................................................... 5
   B. Confidentiality (Section 114) ............................................................................. 7
   C. Complex Circumstances (Section 120) .............................................................. 12
   D. Use of Technology (Sections 200, 220, 300 and 320) ...................................... 14
   E. Close Business Relationships (Section 520, Conforming Amendments in Section 920) 17
   F. Hosting (Subsection 606, Conforming Amendments in Section 900) ................. 19

IV. Other Comments Related to Revisions to the ED ................................................. 20

V. Other Matters ........................................................................................................ 23

VI. Effective Date ....................................................................................................... 25
I. Introduction

1. [Insert December 2022 IESBA vote outcome]

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 that are set out in the final pronouncement.]

3. The proposed 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”).

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), 920 and 950. It also involves revisions to the Glossary to 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.

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.
   - Enhances the Code’s ethical framework to guide the mindset and behavior of professional accountants (PAs) in business and in public practice 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 an 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 PAs, both in business (PAIBs) and in public practice (PAPPs).

9. Since then, the IESBA’s technology project has been 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.”

- The outcome 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
- Comment letter responses to the IESBA Technology Exposure Draft (ED) (see paragraph 13).
- Targeted stakeholder input together with advice from the IESBA Consultative Advisory Group (CAG) and the IESBA’s National Standard Setters (NSS).

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 in relation to 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 of the Code, the Task Force 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 Phase 2 Report.

IAASB-IESBA Coordination

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

- The proposed enhancements preserve the existing consistency in 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, for example, with respect to the fundamental principle of confidentiality, do not require conforming amendments in the IAASB’s International Standard on Quality Management (ISQM) 1 Standard.]
- 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 intentional and appropriate – i.e., the term “technology” encompasses ATT.
- The concepts relating to “complexity” are broadly consistent (i.e., as contained in Part 1 of the Code, and as contained in the IAASB’s International Standard on Auditing (ISA) 315 (Revised 2019), Identifying and Assessing the Risks of Material Misstatement.

¹ The Technology Phase 2 fact finding aimed to identify and assess the potential impact of technology on the behavior of PAs and the relevance¹ 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.
D. Technology Exposure Draft

12. On February 18, 2022 the IESBA issued 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) members, respondents included 6 regulators and audit oversight bodies, 27 PAOs, two independent NSS, nine firms, and four others including the IFAC small and medium sized practitioners’ advisory group (IFAC SMP AG) and an AI software developer.

13. On balance, respondents across stakeholder groups and regions expressed clear support for the Technology proposals. They also suggested drafting improvements and shared some concerns and a number of other comments, including to highlight areas where in their view clarification was warranted to enhance the proposals. The significant issues and principal matters raised by respondents, and the approach taken by the Task Force 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 Consultative Advisory Group (IESBA CAG).
- IAASB Technology Consultative Group.
- International Forum of Independent Audit Regulators Standards Coordination Working Group (IFIAR SCWG).
- International Organization of Securities Commissions 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).

---

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

3 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.

4 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 explicitly emphasize the professional skills that PAs need. The development of the proposal was informed by the International Federation of Accountants’ (IFAC) International Education Standards (IESs) that came into effect on January 1, 2021 and reflect 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.

17. The proposals in the ED reflected the IESBA view that:
   a) The addition of “interpersonal, communication and organizational skills” is generally applicable in the execution of all professional activities and is 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 relevant applicable professional competence standards and resources in order to comply with the requirement in paragraph R113.1.

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. The following substantive comments were raised about the ED proposal - that it:

---

5 Standards of professional competence in the IESs are made available to PAs through their professional accountancy organizations (PAOs), which are subject to IFAC's Statements of Membership Obligations (SMOs). SMO 2 requires compliance with the IESs and other pronouncements developed by the former International Accounting Education Standards Board (IAESB) and issued by IFAC. Paragraphs 5 and 6 of SMO 2 state that:
   - Where IFAC member bodies have direct responsibility, they shall implement all requirements of SMO 2.
   - Where IFAC member bodies have no responsibility for this area they shall use their best endeavors to (a) encourage those responsible for the requirements to follow SMO 2 in implementing them; and (b) assist in the implementation where appropriate.

6 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.
• Appears generic and not technology specific.
• Involves significant judgment and would 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 to the professional activities that they are actually performing, and that there should be effective two-way communication between the team (as a whole) and the client.
• Infers that an apparent lack of “interpersonal, communication and organizational skills” might be considered 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 International Education Standards (IES).

[Task Force Response/ IESBA Decisions]

21. Revisions were made 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 level and type of knowledge and skills needed to perform an activity competently will vary depending on the activity performed. This concept has also been emphasized in revised paragraph 113.1 A3 (extant paragraph 113.1 A2) on maintaining professional competence which requires a PA to have a continuing awareness and understanding of technical, professional, business and technology-related developments. 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. It is further highlighted that such examples are in addition to the application of any technical knowledge relevant to the professional activity.

22. With respect to the fact that the ED proposal is not technology-specific, the Task Force reaffirmed its view 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 is guidance particularly relevant in the technology space as the role of the PA is constantly transforming due to, for example, the automation of routine tasks and emerging applications of technologies in the workplace.

23. Regarding the concern that significant judgment is involved in gauging the degree of competency of the examples of professional skills provided, the Task Force noted that when a PA is identifying the relevant applicable professional competence standards and resources in order to comply with
R113.1, they might consider the IESs which contain detailed factors of what a PA should be able to demonstrate to be considered 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 Task Force views that such detail is more appropriate in non-authoritative guidance which can better elaborate on how these skills are helpful in today’s transformative world.7

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 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” that a PA is required to comply with. This threshold includes information acquired by a PA in the course of their professional or business relationships:

a) In whatever capacity the PA is in (including through “social” gatherings with a client or customer);

b) In any form or medium (e.g., including data, 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 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 laws and/or regulations.

Feedback from Respondents

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

30. Regarding the fundamental principle of Confidentiality more generally, the following principal

---

7 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.
suggestions were raised:

- To clarify whether the fundamental principle of confidentiality still applies where another party puts information in the public domain (including, unlawful disclosure).
- To clarify whether the provisions of Section 114 would prohibit the use of data that had 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 ED glossary definition, the principal points raised included the following:

- Observations that 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 factors 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 obtained at social gatherings, which may or may not be found via search engines online.

[Task Force Response/ IESBA Decisions]

33. The extant Code recognizes that confidentiality serves the public interest because it facilitates the free flow of information from the professional accountant’s client or employing organization to the accountant in the knowledge that the information will not be disclosed to a third party. A PA’s duty of confidentiality is therefore based on this underlying premise as set out in the extant Code. Accordingly, the Task Force has addressed the comments raised in relation to Section 114 against this context.

34. To address comments concerning when confidential information can be used or disclosed more generally, for clarity and consistency, the Task Force developed extant paragraph R114.1 into two separate paragraphs – revised paragraph R114.1 and new paragraph R114.2:

(a) Revised paragraph R114.1 sets out the circumstances under which a PA should respect confidentiality, containing all the sub-bullets of extant paragraph R114.1(a),(b),(c),(g); and

(b) New paragraph R114.2 sets out the circumstances in which a PA cannot use or disclose confidential information, containing all the sub-bullets of extant paragraph R114.1(d),(e),(f).

35. Additionally, new paragraph R114.2:

- Recognizes, in sub-bullet R114.2(a) (i.e., extant sub-bullet (d)), that there are many times where information cannot be disclosed to other individuals within a PA’s own firm or employing organization as well. This is done by withdrawing the extant text “outside the firm or employing organization” at the end of the sub-bullet.
- Outlines the exceptions to the requirement by detailing the specific conditions under which it is possible to use or disclose such information: “(i) there is a legal or professional duty or
right to do so; or (ii) 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."

36. In developing the specific conditions for the exception in paragraph R114.2, the Task Force took into account the existing concepts in the Code, contained in:

   a) Extant paragraph 114.1 A1(b) which stated 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 stated 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."

37. Building on these extant concepts, the new paragraph R114.2 recognizes that laws and regulations will generally not expressly permit use or disclosure of confidential information for specific purposes, and explicitly explains what is meant by proper and specific authority. Accordingly, the specific conditions for use or disclosure of confidential information focuses on whether the specific use or disclosure of confidential information is expressly prohibited by law or regulation, and specifies from whom the authorization to use or disclose confidential information should come from.

Applicability and Interaction with the NOCLAR Provisions

38. The Task Force notes that there is no change in the applicability of the extant Code provisions on responding to non-compliance with laws and regulations (NOCLAR) with respect to Section 114. That is, the NOCLAR provisions are still applicable and "override" Section 114, subject to relevant laws and regulations, and provided that the breach or non-compliance is of such a nature or scale as to meet the public interest test (i.e., being a consideration of whether it has wider public implications in terms of potentially substantial harm to investors, creditors, employees or the general public, in financial or non-financial terms). Under the building blocks approach of the Code, the Task Force affirmed the view that no additional reference to NOCLAR within Section 114 is necessary.

39. Additionally, the Task Force also considered circumstances where a PA faces a dilemma where they have a professional duty to disclose confidential information, for example under the extant Code provisions on responding to non-compliance with laws and regulations (NOCLAR), but where in some jurisdictions, there is no legal protection for the PA in making such disclosure.

40. In such circumstances, the Task Force notes that:

   a) If there is no legal or regulatory prohibition for disclosing confidential information in the public interest, there would be no exposure for breach of the law or regulation; and

   b) The PA needs to consider whether laws or regulations provide protection where a disclosure is made in the public interest.

Accordingly, the PA should consider whether the interests of any other person or entity would be adversely affected such as to give rise to a right to prevent disclosure – for example, because the information is confidential or it might affect the PA’s defense in a criminal prosecution.

41. The Task Force’s view is that this public interest consideration is sufficiently addressed in the first sub-bullet of paragraph 114.2 A2: "In deciding whether to disclose or use confidential information, factors to consider, depending on the circumstances, include… Whether the interests of any parties, including third parties whose interests might be affected, could be harmed if the client or
employing organization authorizes the disclosure or use of information by the PA."

Duty of Confidentiality

42. Regarding comments about a PA’s duty of confidentiality when there is already improper disclosure of information by another party, new sub-bullet R114.2(d) was developed to emphasize that a PA’s duty of confidentiality applies despite such information being publicly available, whether properly or improperly.

43. In developing this new sub-bullet, the Task Force considered:

- Whether information is still considered “confidential” if it has become “properly” available publicly.
  
  In this regard, the Task Force has updated the sub-bullet to refer to "information" not "confidential information" recognizing that once it is publicly available, the information no longer meets the definition of confidential information in the glossary.

- How the sub-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 Task Force views that this is a matter of exercising professional judgment depending on the specific facts and circumstances notwithstanding a PA must uphold its duty of confidentiality in the first instance, unless it has been released or relieved of its duty as outlined in the R114.2.

  For example, a firm might be undertaking a due diligence engagement, and news about such potential transaction might become publicly available. Such publicly available information does not release or relieve the PA of its duty to take appropriate actions to protect the confidentiality of information it has been provided to perform due diligence.

- Whether the phrase “…publicly available, whether properly or improperly” would appear to encompass more scenarios than necessary, for example, including sensitive information which would impact a company’s share price, but for which such information is no longer considered sensitive by the company once a public announcement has been made.

  The Task Force reaffirmed its view that a PA’s duty of confidentiality begins once information is provided to a PA on a confidential basis and continues until permission to disclose or use such information is given by the client or other appropriate authority.

  This approach avoids a PA trying to determine whether disclosure occurred properly or improperly, which would require both knowledge of how the disclosure occurred and any applicable jurisdiction-specific legal considerations.

Use or Disclosure of Confidential Information

44. New paragraph 114.1 A3 has been developed to provide guidance as to when confidential information might be used by PAs, including for purposes such as for AI training or collaborative research.

45. This paragraph also sets out the information that a PA might provide, preferably in writing, to the individual or entity that provided such information, when obtaining authorization to use or disclose confidential information. Specifically, the authorization to be obtained is focused on, and directed at, the individual or entity providing the information. This approach avoids 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, a training organizer, a development or research company, or an entity commissioning a benchmarking survey, etc.).

46. The information that a PA might provide 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, training, development of technology, 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.

47. The Task Force acknowledges that there may be occasions when the identity of the individuals/entities 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 sub-bullet focuses on the need to consider whether the “output of the purpose for which the information is to be used” will protect the identity of the individuals or entities concerned when such output becomes available.

48. The Task Force 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 Task Force 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 decryption. Such risks will have to be assessed and balanced by a PA when anonymizing confidential information.

Other Matters

49. Responsive to other principal points and suggestions raised by ED respondents, the Task Force 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 ED glossary definition of Confidential Information with “is not publicly available” to avoid association with intellectual property rights.
   - Added 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 114.2 A2. This addresses a call 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 Task Force also deliberated if consideration of the laws and regulations regarding where information is stored (i.e., a cloud-based facility) should explicitly be incorporated into the revisions. However, the Task Force notes that paragraph 114.2 A2 is only intended to provide a list of examples for a PA to consider and that it is not possible to explicitly
highlight every circumstance or permutation of law or regulation that might be applicable.

C. Complex Circumstances (Section 120)

Technology ED

50. 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 *Complexity and the Professional Accountant: Practical Guidance for Ethical Decision-making*, to which the Technology Working Group contributed. In particular, the thought leadership 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% respondents supported highlighting complexity as a pervasive factor in decision-making while applying the conceptual framework. 8

51. Taking into account these considerations, the ED proposals reflected the IESBA 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 regard, the guidance should not be restricted to technology-specific complex

---

8 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.
circumstances such as that illustrated in paragraph 23 of the explanatory memorandum to the ED.

Feedback from ED Respondents

52. Support was mixed for these proposals. While some respondents supported the proposals; some respondents did not support 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, 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.
  - The identification and management of complexity would not change the threats and safeguards approach of the Code, nor 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 already included in the conceptual framework.

- The concept of “complexity” in the Code should be aligned with how it is considered in ISA 315 (Revised 2019) 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 which 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 (such as the AI example in paragraph 23 of the ED’s explanatory memorandum).

[Task Force Response/ IESBA Decisions]

53. 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 Task Force considered that there is benefit in retaining some form of guidance on complexity.

54. To address the concerns raised by respondents, revisions were made to the ED to relocate the notion of complexity and incorporate it as part of exercising professional judgment when applying the conceptual framework. Specifically, the revisions build on material contained in extant paragraphs 120.5 A4 and A5 and 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.

55. This approach recognizes that the circumstances in which professional accountants carry out professional activities and the factors involved vary considerably in their range and complexity. It is therefore conceptually aligned with ISA 315 (Revised 2019)’s concept of complexity as “more inherently difficult to apply” to promote consistent application between the ISAs and the Code.

56. 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.

57. In developing the drafting enhancements, the Task Force also debated whether a fact can be uncertain. It was noted that a fact can indeed be uncertain as it may only be a fact at a certain point in time, i.e., it may become a fact or cease to be a fact depending on the information available at a particular point in time.

58. The application material on managing complexity is fundamentally unchanged apart from:
   - The addition, responsive to respondents’ suggestions, of a new factor “analyzing, and investigating, as relevant, any uncertain elements, the variables and assumptions and how they are connected or interdependent,”.
   - Emphasizing that the concepts “being alert” and “communicating inherent uncertainties or difficulties” are already requirements in the Code by cross referencing to the extant paragraphs, responsive to MG member input.

59. Finally, the Task Force considered whether it is appropriate to build in the example contained in paragraph 23 of the explanatory memorandum to the ED but concluded 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. Accordingly, the Task Force reaffirmed its position not to restrict the guidance to a specific technology example, given that the application material is applicable to all circumstances.

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

Technology ED

60. The ED proposals introduced:
   a) Examples of matters to be considered when identifying threats that might arise 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

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

62. With respect to the considerations on identifying threats, the principal points and comments raised were:
   - The matters identified should be linked to specific threats to compliance with the
fundamental principles and that 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 that to use 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., 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 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.

63. With respect to the considerations on 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:

- 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 his/her professional competence and due care obligations.

- The guidance should emphasize the whole process for 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.
o Whether an organization’s general and application controls related to the technology are effective.

o To 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.”

- To further clarify:
  o How the ED sub-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 its reputation, especially where emerging technology is involved.

  o To 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.

  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.

(Task Force Response/ IESBA Decisions)

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

65. The Task Force noted that the examples of “safeguards” provided by respondents are akin to considering the existence of policies, procedures and conditions to evaluate the level of a threat, rather than a “safeguard” as defined by the Code. As such, new paragraphs 200.7 A4 and 300.7 A6 were 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 or firm and its operating environment.

66. 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 noted that the Technology Working Group’s Phase 2 Report highlights considerations for PAs in relation to the use or development of AI systems.

67. 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.

68. As regards the concerns relating to the focus on the “output of the technology,” the Task Force affirmed 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 appropriateness of the inputs to the technology and decisions made by individuals in the course of using 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 employing organization’s or firm’s oversight of the design, development, implementation, operation, maintenance, monitoring, updating or upgrading of the technology.

69. Concerning how a firm or employing organization exercises “oversight” for in-house versus third-party technology, the Task Force 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.

70. Finally, the Task Force 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.

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

Technology ED

71. 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 or licensed by a firm or network firm to an audit client. This reflected the IESBA 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 approach proposed ensures that those users of the Code who look to Section 520 in such circumstances will be guided by the signpost 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/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 (i.e., Section 600) are relevant to the facts and circumstances of the reselling arrangement.

72. The ED also added an example of a technology-related close business relationship and included the concept of “sells” and “resells” to the existing examples of close business relationship 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 close business relationships 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 reflect the IESBA view not to include such 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 that doing so would detract from the principles-based nature of the Code.
Feedback from Respondents

73. Respondents were mainly supportive of the proposed signpost in the ED, although a few respondents did not support 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 non-assurance services and close business relationships are different.
   - The application material gives the impression that pure reselling or selling is a non-assurance service, although that 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.

74. It was also suggested that additional clarity on “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.

75. 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 that contained in paragraph 40 of the explanatory memorandum to the ED – namely 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” and a definition of “business relationship” to be added to the Code, recognizing that the examples provided cannot cover all scenarios.

[Task Force Response/ IESBA Decisions]

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

78. 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 which 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 Task Force debated an observation that it is uncertain whether in all instances a firm will know if the end customer is an audit client of the firm. In this regard, the Task Force views that the firm should know if the end customer is an audit client in most cases, because they will be auditing that client – and therefore have insight into the services/ technology it uses.

79. New application material in paragraph 520.3 A3 addresses, at a principles-based level, respondents’ suggestion to add the example of close business relationships as set out in paragraph 40 of the explanatory memorandum of the ED. In light of the varied nature of these licensing arrangements and how the technology is used, the Task Force explicitly emphasized that such arrangements “might create” a close business relationship and that it “depends on the
specific facts and circumstances." For example, the Task Force observes 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.

80. The Task Force 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 and impractical to add all examples of technology-related close business relationships.

81. With respect to the calls to add a general principle for identifying or assessing close business relationships or adding a definition of business relationships, the Task Force noted that it is out of the scope of the technology project, but that such feedback can inform a potential future workstream to comprehensively review Section 520, which is being considered in the development of the consultation paper pertaining to IESBA’s 2024-2027 strategic work plan.

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

Technology ED

82. The ED proposals set out examples of assuming management responsibility in relation to IT systems services and are therefore prohibited for all audit clients (ED paragraph 606.3 A1). The proposals further expand on the prohibition on assuming management responsibilities in extant paragraphs R400.15 and revised paragraph R606.3.

83. The ED position reflects 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.

84. However, the proposals acknowledge 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

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

   • 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 is intended to cover:

     o 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 that the examples should give consideration to the type of data being hosted, the method of hosting, and the purpose of the hosting.

- Suggestions that the phrase “directly or indirectly” should be expanded on in the Code, (i.e., as it was in paragraph 52 of the explanatory memorandum to the ED).

[Task Force Response/ IESBA Decisions]

86. Revisions were made to the ED paragraph 606.3 A1 to address the comments raised by respondents. In particular:

- The phrase “services in relation to hosting” in the ED lead-in has been replaced with “stores data or manages” to be more specific as to the type of hosting services covered by the prohibition.

- Sub-bullets (a) to (c) were added, 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).

87. The Task Force’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 it is conducted either directly on internal servers or indirectly on a cloud provider’s server.

88. Regarding the ED paragraph 606.3 A2, the term “transmission” has been added to highlight that portals for transferring information in the course of providing a permissible service are not prohibited. The term “in the course of an audit” has also been added for avoidance of doubt that transmission of information in such circumstances is not precluded.

89. Finally, the Task Force 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 non-assurance services. However, since the material is specific to examples of IT systems services that result in the assumption of a management responsibility, the Task Force views that it is appropriately positioned under the overarching requirements and application material relating to the prohibition on assuming management responsibility. Relocating such material into Section 950 would have the consequence of needing 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, as Section 606 is).

IV. Other Comments Related to Revisions to the ED

90. Other revisions arising from the Task Force’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 that questioned what sufficient information would consist of, and who is in a position to judge its sufficiency; the Task Force 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 Code 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 of a PA to “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 revisions 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 term was replaced 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. That term has therefore been replaced with “entities” to broaden its scope.
• Update extant paragraph 200.5 A3 to reflect the broadened expectations of ethical leadership.

95. Finally, new paragraph 300.5 A2 was added 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 (NAS) 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 reflects the IESBA’s position that such guidance encompasses

• All the possible ways through which a firm or a network firm might perform a NAS, including, for example, when a firm’s staff uses third-party software to perform the NAS, or when a firm uses technology to perform the NAS.
• Where a firm or a network firm provides, sells, resells or licenses technology to an audit client.

97. Responsive to respondents, the revisions add 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 elaborates on the IESBA 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 assumption of management responsibilities in Section 400. This material further emphasizes 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 revisions take 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 Task Force acknowledges the overlap but considers no change is necessary given that “routine or mechanical” is a long-standing phrase that has been widely used and understood to date. 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 phrase, might cause confusion to users of the Code.

- Whether the application material in ED paragraph 400.16 A1 is necessary, and whether such material is overly broad – i.e., it would appear to cover technology such as email. The Task Force reaffirmed its view 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 Task Force further reaffirmed its view that the revisions apply to all technology, ranging from e-mail to AI.

IT Systems Services and Self-review Threat

101. The ED proposals modernized and strengthened 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:

- Expands 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.

- Provides additional examples of IT systems services that might create a self-review threat and are therefore prohibited for PIE audit clients.

- Withdrew the extant approach for the provision of services involving the implementation of certain “off-the-shelf” accounting or financial information 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.

102. The revisions reflect drafting refinements which take into account respondents’ suggestions. In addition, the revisions give explicit consideration to cyber-security which is increasingly relevant in today’s world, and addresses 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.

103. The Task Force was careful to balance the public interest elements of providing such services to small-medium enterprises versus prohibiting such services due to the creation of the self-review threat. Therefore, for non-PIEs audit clients, such services are still permissible provided the appropriate safeguards are in place. For PIE audit clients, such services are prohibited.

104. Finally, the Task Force is cognizant that there are some cybersecurity services requested by a client that – depending on the facts and circumstances – might be akin to the provision of advice and recommendations. In this regard, the Task Force reaffirmed its view 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 – but that the firm 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

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

• Added an explicit statement 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.”

106. Regarding certain types of IT systems services that might create a self-review threat, the revisions add an additional example to the ED proposal. As suggested by respondents’ this example explicitly considers the “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 Task Force believes this to be particularly relevant given the exponential rise in sustainability-related services.

V. Other Matters

107. Other substantive matters raised by respondents’ and considered by the Task Force are set out below.

Documentation Expectations

108. Respondents questioned what are the PA’s documentation expectations in relation to the revisions pertaining to Parts 1 to 3 of the Code.
109. The Task Force 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.

110. In this regard, it was noted that the need for documentation is not a consideration that arises only in relation to the use of technology, and that the IESBA had 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.

**Applicability of the Revisions to Multidisciplinary Teams**

111. Respondents questioned how PAs might apply the revisions in Parts 1 to 2 of the Code since it would 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, including maintaining confidentiality.

112. To this end, the Task Force 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, including 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.

113. Additionally, the Task Force also observes 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 PAs’ ability to obtain information in relation to the factors required to determine whether to use the work of others or the output of technology.

114. Finally, the Task Force noted that the IESBA’s imminent work plan also involves a holistic review to expand guidance on the use of others/ experts (i.e., from both the ethics and independence perspectives). This workstream is anticipated to commence in 2023.

**Applicability of the Revisions to All Technologies**

115. Respondents questioned whether the revisions apply to all types of technology, such as that ranging from e-mail, excel, to AI, blockchain, etc.

116. In this regard, the Task Force reaffirmed its position that the revisions should apply to all technologies. This is important as the revisions have been developed in a principles-based manner in order to ensure the relevance of the Code as technology evolves.
117. Accordingly, the use of the term “technology” in the proposals is broad and is meant to encompass all technologies (including “automated tools and techniques” as used in the auditing standards, AI and machine learning, blockchain, and other future technologies not yet known).

118. PAs should therefore exercise professional judgment when determining the level of knowledge, understanding, oversight, etc., that might be required to use technology. Common use (i.e., excel) does not preclude threats to the fundamental principles, depending on facts & circumstances.

Potential Implementation Challenges for Small-medium Practitioners or Enterprises

119. Respondents suggested that the Task Force consider implementation challenges or unintended consequences for small-medium practitioners or enterprises. For example, segregation of duties concerns due to resource or cost constraints.

120. The Task Force has taken such considerations into account. Specifically, the ED was developed with input arising from outreaches with the IFAC small-medium practitioners’ advisory group (IFAC SMP AG), as well as the Technology Working Group’s fact-finding work, which included outreaches with PAIBs within small-medium enterprises. The revisions also consider input from the IFAC SMP AG comment letter to the ED.

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

121. Respondents commented on the Code’s pace of change, length and increasing requirements. The Task Force noted that this is not a new concern, and that the IESBA will consider this broader, strategic matter as it develops its 2024-2027 strategic work plan.

122. Nevertheless, as it relates to technology – the IESBA’s technology workstreams were designed to address the challenge of evolving technology transformation – instead of trying to keep pace and change the Code with every new technology; the focus was to develop and issue principles-based revisions to the Code that apply to all technologies, as a priority. It is viewed that such revisions will future-proof the Code as advancements in technology continue.

123. The IESBA will now shift to focusing on monitoring technology developments on the ground, allowing time for these revisions to be adopted and for stakeholders to undertake the necessary implementation efforts. This shift is complemented and 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 transformation 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.

124. 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

125. As discussed above, some respondents to the ED pointed to the Code’s pace of change, length and increasing requirements.

[Task Force Response/ IESBA Decisions]

126. The Task Force’s view is that the effective date should be as follows, with no transitional provision:

- 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.

127. In determining the effective date for the revisions, the Task Force sought to balance (i) the public interest benefit of having the revisions take effect as soon as practicable, and (ii) the need for a sufficient period to enable awareness of the revisions to be promoted, and for adoption, and implementation at firm and jurisdiction levels to take place.

128. The Task Force has considered the following:

- The objective 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 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 targeted national standard-setters that there should be a reasonable timeframe which allows for translation, jurisdiction specific due processes for adoption, and the development of appropriate implementation infrastructure to take place.

---


10 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 be faced with the challenge of terminating the provision of such services, with the consequential disruption and associated practical issues for the client.