

Exposure Draft
February 2022
Comments due: June 20, 2022

*International Ethics Standards Board
for Accountants®*

Proposed Technology-related Revisions to the Code

IESBA

International
Ethics Standards
Board for Accountants®



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 Federation of Accountants® (IFAC®).

Copyright © February 2022 by the International Federation of Accountants (IFAC). For copyright, trademark, and permissions information, please see [page 77](#).

REQUEST FOR COMMENTS

This Exposure Draft, [Proposed Technology-related Revisions to the Code](#), was developed and approved by the IESBA.

The proposals in this Exposure Draft may be modified in light of comments received before being issued in the final pronouncement. Comments are requested by **June 20, 2022**.

Respondents are asked to submit their comments electronically through the IESBA website using the "[Submit a Comment](#)" link. Please submit comments in both PDF and Word files. Also, please note that first-time users must register to use this feature. All comments will be considered a matter of public record and will ultimately be posted on the website. Although the IESBA prefers that comments are submitted via its website, comments can also be sent to Ken Siong, Program and Senior Director, at KenSiong@ethicsboard.org.

This publication may be downloaded from the IESBA website: www.ethicsboard.org. The approved text is published in the English language.

PROPOSED TECHNOLOGY-RELATED REVISIONS TO THE CODE
CONTENTS

| | Page |
|---|------|
| EXPLANATORY MEMORANDUM | 5 |
| I. Introduction | 5 |
| II. Background and Overview | 5 |
| III. Significant Matters – Fundamental Principles (Parts 1 to 3)..... | 10 |
| IV. Significant Matters – Independence (Parts 4A and 4B) | 17 |
| V. Analysis of Overall Impact of the Proposed Changes | 21 |
| VI. Project Timetable and Effective Date | 21 |
| VII. Guide for Respondents..... | 22 |
| EXPOSURE DRAFT: PROPOSED TECHNOLOGY-RELATED REVISIONS TO THE CODE | 25 |

EXPLANATORY MEMORANDUM

I. Introduction

1. This memorandum provides background to, and an explanation of, the proposed technology-related revisions to the [International Code of Ethics for Professional Accountants \(including International Independence Standards\)](#) (the Code).
2. The IESBA approved these proposed changes for exposure at its November-December 2021 meeting.

II. Background and Overview

A. Project Objective and Scope

3. 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 also with strategic input from the Public Interest Oversight Board (PIOB). The project involves a review of the Code to determine technology-related revisions that are necessary for the Code to continue to remain relevant and fit for purpose in response to the transformative effects of major trends and developments in technology on the work of the global accountancy profession.
4. The technology project was approved in March 2020, and has been informed by various inputs, including:
 - (a) A Working Group¹ [Report](#) which was issued in February 2020 (Phase 1 Report), and summarized the IESBA's 2018-2019 fact-finding and research on the impact of trends and developments in artificial intelligence (AI), big data, and data analytics on the ethical behavior of professional accountants, both in business (PAIBs) and in public practice (PAPPs). The Report outlined seven areas ("recommendations") that formed the basis of the IESBA's [Technology Project Proposal](#).
 - (b) Stakeholder [responses](#) to two Technology [Surveys](#) issued by the Technology Task Force in October 2020 on the topics of "Technology and Complexity in the Professional Environment" and "The Impact of Technology on Auditor Independence."
 - (c) Technology-related feedback on the January 2020 Non-Assurance Services (NAS) [Exposure Draft](#) that the IESBA determined would be addressed by the Technology Task Force.²
 - (d) Continued stakeholder input, including from over 50 targeted outreach meetings and events involving a broad range of stakeholder groups across many geographies; the IESBA's Consultative Advisory Group (CAG); the IESBA-National Standard Setters Liaison Group (NSS); the Forum of Firms (FoF); IFAC's Small and Medium Practices Advisory Group (SMP AG); and certain members of the Monitoring Group (i.e., the International Organization of Securities Commissions (IOSCO) and the International Forum of Independent Audit Regulators (IFIAR)).

¹ The 2019 Technology Working Group was chaired by former IESBA Member Patricia Mulvaney, and included members Greg Driscoll, IESBA Technical Advisor, Brian Friedrich, IESBA Member, Hironori Fukukawa, IESBA Member, and Myriam Madden, former IESBA Member.

² When the IESBA approved the NAS revisions to the Code in December 2020, the IESBA determined that technology-specific matters should be addressed as part of the Technology project (see pages 7-8 and paragraphs 102, 103, 124 and 125 of the [NAS Basis for Conclusions](#)). Section IV, A-D of this Explanatory Memorandum explains how the proposals have addressed such matters.

5. The proposals incorporate input from IESBA deliberations dating back to June 2020 in the course of which the IESBA considered findings in the Phase 1 Report, including the seven recommendations. As part of its deliberations, the IESBA considered whether some of the concepts underlying the recommendations are already incorporated and inherent in the fundamental principles of the Code, as revised by the [role and mindset revisions](#) to the Code (see paragraph 7 below).

B. About the Proposed Revisions

6. The proposed technology-related revisions are to the most current version of the Code (“extant Code”), including all revisions that will become effective in December 2022 (i.e., [revisions relating to the objectivity of an engagement quality reviewer and appropriate reviewers](#), and the [revised NAS](#) and [fee-related provisions](#) of the Code).³ The proposals also take into account the revisions that the IESBA approved in December 2021 that are subject to PIOB approval (i.e., the quality management-related conforming amendments to the Code, and the revisions relating to the Definitions of Listed Entity and Public Interest Entity (PIE)).

Recently Issued Pronouncements that Apply in Technology-Related Circumstances

7. The technology-related revisions build on recent revisions to the Code, including those arising from the Role and Mindset and NAS projects. The revisions resulting from these projects introduced changes to the Code that are relevant to technology. In particular:
- The role and mindset revisions, which became effective on December 31, 2021:
 - Note that maintaining professional competence requires a continuing awareness and an understanding of relevant technical, professional, business and **technology-related** developments (see paragraph 113.1 A2).
 - Acknowledge that a professional accountant’s (PA) exercise of professional or business judgment can be compromised by undue influence of, or undue reliance on, individuals, organizations, **technology** or other factors (see paragraph 110.1 A1).
 - Highlight that conscious or unconscious **bias** affects the **exercise of professional judgment** when identifying, evaluating and addressing threats to compliance with the fundamental principles. Those revisions also provide examples of bias. (See paragraphs 120.12 A1 to 120.12 A2.) Most relevant is **automation bias**, which is a tendency to favor output generated from automated systems, even when human reasoning or contradictory information raises questions as to whether such output is reliable or fit for purpose.
 - The revised NAS provisions that will become effective for audits of financial statements for periods beginning on or after December 15, 2022:
 - Prohibit firms from providing IT systems services to audit clients that are PIEs if the provision of such services might create a self-review threat (see paragraph R606.6).
 - Provide examples of services that are prohibited because they give rise to a self-review

³ To access the Code and to obtain final pronouncements issued subsequent to April 2021, visit the IESBA’s website at: www.ethicsboard.org/standards-pronouncements.

threat. Such examples include the provision of services to PIE audit clients that involve designing or implementing *IT systems* that (a) form part of the internal control over financial reporting, or (b) generate information for the client's accounting records or financial statements on which the firm will express an opinion (see paragraph 606.6 A1).

C. Highlights of Proposed Technology-related Revisions

8. The proposed technology-related revisions to the extant Code have been developed in a principles-based manner in order to preserve the relevance of the Code as technology evolves.⁴ Accordingly, the use of the term “technology” in the proposals is broad and is meant to encompass all technologies (including AI and machine learning, blockchain, and other future technologies not yet known).
9. In developing the proposed technology-related revisions, the IESBA reviewed and considered the entire Code, including the independence provisions.

Part 1 – Complying with the Code, Fundamental Principles and Conceptual Framework

10. Key proposed revisions to Part 1:
 - Expand on the extant Code (including the role and mindset revisions) to acknowledge further technology-related considerations in describing the fundamental principles of professional competence and due care and confidentiality (see proposed revisions to paragraphs 113.1 A1, R113.3, 114.1 A3; and proposed paragraph 114.1 A1 and the glossary).
 - Provide additional considerations to assist in applying the conceptual framework, including:
 - A recognition that public trust is driven in part from a PA's ethical behavior in professional or business relationships, which might involve technology-related facts and circumstances (see proposed revisions to paragraph 120.14 A3).
 - A discussion of complex circumstances and why these circumstances are a consideration in applying the conceptual framework. The discussion includes a description of the facts and circumstances involved when complex circumstances arise and provides guidance to assist PAs manage such circumstances or mitigate their impact (see proposed paragraphs 120.13 A1 to A3).

Parts 2 and 3 – Professional Accountants in Business and Professional Accountants in Public Practice

11. Within Parts 2 and 3 of the Code, the proposals:
 - Provide new application material to assist in identifying threats to compliance with the fundamental principles when a PA uses or relies upon the output from technology (see proposed paragraphs 200.6 A2 and 300.6 A2).
 - Provide guidance to assist PAs when they rely on, or use, the output of technology. In particular, the proposals include a range of factors and other considerations intended to guide such thinking

⁴ The [Phase 1 Report](#), which states that “generally, the Code currently provides high level, principles-based guidance for most technology-related ethics issues that PAs and firms might encounter,” supports this principles-based approach.

(see proposed revisions to paragraphs R220.7 and R320.10, and proposed paragraphs 220.7 A2, 220.7 A3 and 320.10 A2).

Parts 4A and 4B – International Independence Standards (IIS)

12. In the case of the independence provisions that apply to audit and review engagements, the proposals:
- Include clarifications and refinements to the revised NAS provisions that were issued in April 2021. In particular, proposed revisions are being made to revised Section 600 to:
 - Clarify that the NAS provisions apply (i.e., firms should consider the relevance of such provisions) in circumstances where technology is used by a firm or network firm to provide a NAS to an audit client, or where a firm or network firm provides, sells, resells or licenses technology to an audit client (see proposed paragraphs 600.6 and 520.7 A1).
 - Explicitly draw out that the client’s dependency on the service, including the frequency with which the service will be provided, is relevant in identifying the different threats that might be created by providing a NAS to an audit client, and in evaluating the level of such threats (see proposed third bullet of paragraph 600.9 A2).
 - Provide a description of IT systems services that is broad in scope and goes beyond design and implementation (see proposed paragraph 606.2 A1). There is also enhanced clarity about the examples of IT systems services that:
 - Result in the assumption of a management responsibility for an audit client (e.g., services relating to hosting of an audit client’s data) and therefore are prohibited (see proposed paragraphs 606.3 A1 to 606.3 A2).
 - Might create a self-review threat (e.g., implementing accounting or financial information reporting software) (see proposed paragraph 606.4 A3). In the case of audit clients that are PIEs, such services are prohibited.
 - Withdraw the presumption in extant paragraph 606.4 A2 that providing certain IT system services⁵ does not usually create a threat as long as individuals within the firm or network firm do not assume a management responsibility.
 - Acknowledge that accounting and bookkeeping services can either be manual or automated and provide new application material to prompt firms’ consideration of how the technology functions and whether the technology is based on expertise or judgments of the firm or a network firm when determining whether an automated accounting or bookkeeping service is “routine or mechanical” (see proposed paragraph 601.5 A2 and proposed revisions in paragraph 601.5 A3). There is also enhanced clarity on the prohibition on assuming management responsibilities to emphasize that when technology is used in performing a professional activity for an audit client, the requirements in paragraphs R400.15 and R400.16 apply regardless of the nature or extent of such use (see proposed paragraph 400.16 A1).
 - Provide enhanced clarity about the nature of technology-related arrangements that create a close

⁵ For example, implementing “off-the-shelf” accounting and financial information reporting software that was not developed by a firm or a network firm, if the customization required to meet the client’s needs is not significant.

business relationship (see proposals in paragraph 520.3 A2).

13. In the case of the independence provisions that apply to assurance engagements other than audit and review engagements, the proposals:
- Clarify, by an explicit statement that “[Part 4B of the Code] applies to assurance engagements on an entity’s non-financial information, for example, environmental, social and governance (ESG) disclosures” (see proposal in paragraph 900.1).
 - Include proposed amendments that are intended to preserve the existing alignment between Parts 4A and 4B of the Code (see proposed paragraphs 900.14 A1, 920.3 A2, 920.6 A1, 950.5 and 950.7 A2 third bullet).
 - Provide an example of a technology-related NAS that might create a self-review threat⁶ in relation to the subject matter information of an assurance engagement, and examples of certain technology-related professional activities that involve the assumption of management responsibility in relation to the underlying subject matter and, in an attestation engagement, the subject matter information of an assurance engagement (see proposed paragraphs 950.10 A1 and 900.13 A4 and A5).

D. Interactions with Other IESBA Work Streams and the IAASB

Technology Working Group

14. In addition to its Technology Task Force (which is responsible for the proposed revisions in this Exposure Draft), the IESBA has established a new Technology Working Group. This Working Group is responsible for:
- Developing or facilitating thought leadership and other materials⁷ that highlight technology trends and developments and the resulting ethics (and independence) implications for PAs.
 - Undertaking fact-finding to identify and assess the potential impact of technology developments⁸ on the accountancy profession.
15. The Technology Working Group’s work is still ongoing. However, it has shared relevant insights and observations with the Task Force and these were considered in developing the technology-related proposals. The IESBA determined that it is appropriate for the proposals to be issued now given that they are largely principles-based. In addition, while the IESBA remains committed to pursuing fact finding on developments in technology and understanding their implications from a standard-setting perspective, there is a public interest need for timely enhancements to the Code given the rapid pace of change in, and use of, technology (see paragraphs 58 to 59 below).

⁶ As proposed, the technology-related services that might create a self-review threat relate to “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.”

⁷ This IESBA’s [Technology Focus Webpage](#) includes a compilation of the various thought leadership and other resource materials that have developed or considered by the Technology Working Group. This compilation is continually being updated as new material is developed/ identified.

⁸ The scope of the Technology Working Group’s work is broad. In addition to the topics covered in the Phase 1 Report (i.e., AI, big data, and data analytics), this work also covers topics such as blockchain, cybersecurity, and cloud computing.

IAASB-IESBA Coordination Matters

16. In developing the proposals, the IESBA coordinated 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](#).

III. Significant Matters – Fundamental Principles (Parts 1 to 3)**A. Identifying Threats Arising from the Reliance on the Output of Technology**

17. The proposals explain that use of technology is a specific circumstance that might create threats to compliance with the fundamental principles. They provide considerations to help in identifying threats that might arise when PAs rely upon the output from technology (see proposed paragraphs 200.6 A2 and 300.6 A2). The proposed application material sets out the following considerations to help in identifying such threats and is intended to support the proper application of the conceptual framework and complement the overarching provisions in Section 120:

- Whether information about how the technology functions is available to the PA.
- Whether the technology is appropriate for the purpose for which it is to be used.
- Whether the PA has the professional competence to understand, use and explain the output from the technology.
- Whether the technology incorporates expertise or judgments of the PA or the employing organization.
- Whether the technology was designed or developed by the PA or employing organization and therefore might create a self-interest or self-review threat.

18. The IESBA deliberated whether such application material might be located within Section 120 but ultimately determined that consistent with the Code's building blocks approach, the appropriate location for the new application material is both Parts 2 and 3 of the Code. This is because the guidance sets out additional provisions for applying the conceptual framework for PAIBs (i.e., Section 200) and PAPPs (i.e., Section 300). The IESBA believes that placing this guidance in Sections 200 and 300 will make the considerations more visible to PAIBs and PAPPs and will better assist them in identifying threats that might arise from reliance on the output from technology.

B. Relying on the Work of Others or on the Output of Technology

19. The proposals provide examples of factors for PAIBs and PAPPs to consider in determining whether reliance on or use of the output of technology is reasonable or appropriate for the intended purpose (see proposed paragraphs 220.7 A2 and 320.10 A2). Among others, such factors include:
- The PA's ability to understand the output from the technology for the context in which it is to be used.
 - Whether the technology is established and effective for the purpose intended.
 - Whether new technology has been appropriately tested and evaluated for the purpose intended.

- The appropriateness of the inputs to the technology.

The IESBA noted that inputs to technology are not only data, but also other information such as decisions made by individuals relating to the operation of the technology (see last bullet of proposed paragraphs 220.7 A2 and 320.10 A2).

20. The IESBA considered possible circumstances where it might not be feasible for a PAIB to be able to determine whether the reliance on the output of technology is reasonable, for example, where “junior level” PAIBs might be asked to perform a task without the ability to obtain the information to determine the reasonableness of such reliance. To address this, proposed paragraph 220.7 A3 acknowledges that a PAIB’s position in an employing organization impacts the PAIB’s ability to obtain information in relation to the factors required to determine whether reliance on the work of others or on the output of technology is reasonable.

C. Consideration of “Complex Circumstances” When Applying the Conceptual Framework

21. PAs might find themselves working in complex circumstances brought on by, amongst other factors, the impact of new technologies. Also, 82% of respondents to the [Technology and Complexity in the Professional Environment](#) survey expressed support for having more guidance in the Code to help PAs navigate complex circumstances. The IESBA determined that the existence of complex circumstances is a consideration in applying the conceptual framework, but not a new category of threat. Accordingly, the proposals include a discussion of complex circumstances in proposed paragraphs 120.13 A1 to 120.13 A3. Among other matters, this new application material:

- Recognizes that some professional activities might involve complex circumstances that increase the challenges when identifying, evaluating and addressing threats to compliance with the fundamental principles.
- Explains the relevant facts and circumstances that give rise to complex circumstances.
- Provides guidance to help PAs manage these complex circumstances and mitigate the resulting challenges.

22. The IESBA’s view is that complex circumstances involve (a) elements that are uncertain, and (b) multiple variables and assumptions, which are interconnected or interdependent (see paragraph 120.13 A2 (a) and (b)). The IESBA determined that the characteristics described in proposed sub-paragraphs 120.13 A2 (a) and (b) would always need to be present when complex circumstances arise. The IESBA acknowledges that other conditions might be present when complex circumstances arise, such as rapidly changing facts and circumstances, but is of the view that these other conditions are not determinative as to when a complex circumstance arises.

Complex Circumstances – Broad Versus Specific Provisions

23. In finalizing the proposals, the IESBA acknowledged that complex circumstances have always existed and are not a new phenomenon specific to technology. However, the IESBA observes that rapid digitalization has increased the interconnectedness of social, economic, and geopolitical systems, which

is a complex circumstance that PAs are now facing.⁹ In this regard, the IESBA considered whether the proposed facts and circumstances involved when complex circumstances arise should be specific to technology, for example, to:

- Highlight that the use of machine learning-based AI models is complex because it is dependent on multiple data inputs that collectively impact the machine learning in uncertain ways that might render the output unpredictable (i.e., meeting the description in proposed paragraph 120.13 A2). In particular, the IESBA noted that the volume of data inputs that drive the pace of machine learning might render it a “black box” scenario and might impact a PA’s ability to keep up with understanding and explaining the AI outputs.
- Emphasize why the actions listed in proposed paragraph 120.13 A3 are important to manage the complexity of AI outputs.¹⁰ For example, monitoring any developments or changes in the AI outputs and consulting with experts might help the PA assess the reasonableness of such outputs before a “black box” scenario is created.

24. Focusing on ensuring that the Code remains relevant and fit-for-purpose, the IESBA determined not to restrict the proposed provisions relating to complex circumstances to technology-specific situations. In arriving at this determination, the IESBA was mindful of the plethora of non-technology examples pertaining to complex circumstances provided by survey respondents¹¹ (e.g., rapidly changing laws and regulations with differing public interest angles from a jurisdictional versus global perspective).

The Term “Complex”

25. It has been drawn to the IESBA’s attention that, in some jurisdictions, the same word might be used to translate “complex” and “complicated.” As the IESBA’s intention in including proposed paragraphs 120.13 A1 to A3 is to highlight the particular considerations that give rise to complex circumstances, the IESBA is seeking input as to jurisdictions where this issue might arise and how, in such jurisdictions, the term ‘complex’ is translated.
26. Apart from translation considerations, the IESBA also noted that ‘complex’ and ‘complicated’ are often used interchangeably by the general public and anticipates that some PAs might turn to the new application material on complex circumstances whenever ‘unclear’, ‘difficult’, ‘complicated’ or ‘complex’ circumstances are encountered. In this regard, the IESBA believes that there will not be a downside to a PA considering the actions to manage complex circumstances in addition to applying the conceptual framework.

⁹ For example, see thought leadership on [Ethical Leadership in an Era of Complexity and Digital Change](#), which includes contributions from the Technology Working Group.

¹⁰ In the scenario where a PA is relying on, or using, the output of AI models, proposed paragraphs 200.6 A2 and 300.6 A2 also contain considerations relevant when identifying threats to compliance with the fundamental principles. Proposed paragraphs 220.7 A2 and 320.10 A2 contain factors to consider when relying on or using the output of AI.

¹¹ Paragraphs 7 and 8 of the [Summary of Technology Survey Results](#).

D. Professional Competence and Due Care

27. Building on the extant Code (including the role and mindset revisions), the proposals highlight the importance of non-technical professional skills needed by PAs in the digital age (i.e., “soft” skills) with the proposed revisions in paragraph 113.1 A1. The proposals take into account the following:
- The International Federation of Accountants’ (IFAC) recently revised International Education Standards (IESs) that came into effect on January 1, 2021, which already reflect the increasing demand for PAs to be skilled in information and communications technologies. Specifically, the IESBA’s proposals incorporate language to emphasize the importance of the interpersonal, communication, and organizational skills as outlined in [IES 3: Professional Skills](#).¹²
 - The execution of professional activities generally requires the application of soft skills, and this is not specific to technology-related circumstances. The IESBA noted that soft skills are increasingly regarded as critical for the future-ready PA. Concepts such as “growth mindset,” “having an inquiring mind,” and “exercising professional judgment” formed part of the IESBA’s deliberations in finalizing the role and mindset revisions. They are also reflected in the provisions set out in [IES 4: Professional Values, Ethics, and Attitudes](#).¹³ In this regard, the IESBA determined that IES 4 and the remainder of the specific learning outcomes in IES 3 paragraph 7 relating to intellectual skills (e.g., critical thinking, adaptability), and personal skills (e.g., commitment to lifelong learning) are already incorporated in the Code (i.e., as part of the role and mindset revisions).
28. The IESBA noted that some representatives of IFAC’s International Panel on Accountancy Education (IPAE) expressed support for the proposed revisions in paragraph 113.1 A1, and a preference for the inclusion of a reference to IESs or equivalent education standards.

¹² 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.

¹³ Skills defined in learning outcomes for IES 4, paragraph 11 are (a) Professional skepticism and professional judgment, (b) Ethical principles, and (c) Commitment to the public interest.

Consideration of a Reference to Standards of Professional Competence in the Code

29. The IESBA considered and on balance determined not to include guidance such as the following in the Code to explicitly refer PAs to standards of professional competence, for example, those in the IESs:

113.1 AX Standards of professional competence, such as those in the International Education Standards, are implemented through the professional competency requirements of individual jurisdictions.

30. In weighing whether to include such guidance, the IESBA noted that the extant Code includes an implicit obligation for PAs to identify the relevant applicable professional competence standards and resources in order to comply with the requirement in paragraph R113.1, appropriately informed by the guidance in paragraph 113.1 A2.¹⁴
31. The IESBA's position is consistent with the approach that the IAASB took in finalizing its International Standard on Quality Management (ISQM) 1, [Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements](#). In particular, ISQM 1 paragraph A88 aligns with the terminology utilized in the IESs but does not make an explicit reference to the IESs as an example of standards of professional competence.
32. Finally, the IESBA notes that 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 \(SMOs\)](#).¹⁵ In this regard, a PAO's initial professional development programs for aspiring accountants and continuing professional development programs for PAs will be based on the relevant professional competency standards to enable PAs to meet the relevant professional competency requirements.

E. Confidentiality and Confidential Information

33. The proposals explain how PAs maintain the confidentiality of information acquired in the course of professional and business relationships. In particular, they include an explicit prompt for PAs to secure such information in the course of the entire data governance cycle (i.e., from data generation or collection through to their use, transfer, storage, dissemination and lawful destruction) (see proposed paragraph 114.1 A1). In this regard, the IESBA is proposing a new definition of "Confidential Information" in the Glossary. The IESBA believes its proposals are particularly relevant in light of today's data-driven world and the ease with which data are accessible. In addition, the proposals include refinements to enhance the flow of the provisions in Section 114 and to modernize the language used in the last two bullets in

¹⁴ Extant paragraph R113.1 requires PAs to "attain and maintain professional knowledge and skills...based on **current technical and professional standards and relevant legislation**" and "act diligently and in accordance with **applicable technical and professional standards**". Paragraph 113.1 A2 explains that "**continuing professional development** enables a professional accountant to develop and maintain the capabilities to perform competently within the professional environment."

¹⁵ [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.

paragraph 114.1 A3 (e.g., “type of communication and to whom it is addressed” is changed to “means of communicating the information”).

34. The IESBA’s proposed definition of confidential information is broad and includes “any information, data or other material in whatever form or medium (including written, electronic, visual or oral) that is not in the public domain.” The proposed definition is intended to encompass all the possible scenarios in which information might be obtained and establishes a threshold for confidential information (i.e., information that is not in the public domain). The approach mitigates the risk of having varying levels of subjectivity to determine what constitutes confidential information. In addition, what constitutes confidential information should not be impacted by the capacity in which the PA receives the information.

F. Consideration of Terminology in Existing AI Ethics Guidance

35. The IESBA considered whether the terminology included in different sources of AI ethics guidance (e.g., accountability, transparency, explainability and privacy) should be leveraged for inclusion in the Code to minimize unnecessary differences that might detract from understanding ethics issues that might arise from the use of emerging technologies that involve AI and machine learning. In this regard, the Phase 1 Report included a comparison of common principles used in five different AI Ethics guidelines¹⁶ to the Code’s five fundamental principles of ethics and concluded that generally, the Code currently provides high level, principles-based guidance for most technology-related ethics issues that PAs and firms might encounter.

36. The IESBA believes that the concepts underlying the terminology used in the various sources of AI Ethics guidelines are sufficiently incorporated in the proposed technology-related revisions to the Code. For example, the terms:

- (a) **Accountability** – The concepts in the guidelines explaining the term “accountability” are addressed in the proposals that set out relevant considerations in identifying threats to compliance with the fundamental principles when PAs rely on the output of technology (see proposed paragraphs 200.6 A2 and 300.6 A2); and in the examples of factors that PAs are to consider in determining whether the use of, or reliance on, the output of technology is reasonable (see proposed paragraphs 220.7 A2 and 320.10 A2). Although PAs do not need to be experts in technology, the IESBA anticipates that they will have a reasonable degree of awareness and understanding of certain matters with a view to deciding whether reliance on the output of technology is reasonable.
- (b) **Transparency and Explainability** – The IESBA’s current thinking is that “transparency” and “explainability” are related concepts. Transparency refers to the extent of being able to understand how a system functions or a decision was made, whereas explainability involves the ability to explain, and so understand, why a system produced certain outputs or a decision-maker’s rationale for decisions made.

The key concepts set out in the descriptions of “transparency” and “explainability” in the AI guidelines are covered by the proposed revisions in paragraph R113.3 and proposals in paragraphs 120.13 A3, 200.6 A2, 220.7 A2, 300.6 A2 and 320.10 A2. For example, those proposals include:

¹⁶ The Phase 1 Report compared five different sets of AI Ethics guidelines to the Code, namely those issued by Microsoft, IBM, the European Commission, the Organisation for Economic Cooperation and Development (OECD), and the Australian Government.

- Making clients, the employing organization or other users of the PA’s professional services or activities *aware* of the limitations inherent in the services or activities and providing them with *sufficient information to understand* the implications of those limitations.
 - Considering whether information about *how* the technology functions is available to the PA.
 - Considering whether the technology is *appropriate for the purpose* for which it is to be used.
 - Considering whether the PA has the professional competence to *understand, use* and *explain* the output from the technology.
 - Considering the PA’s ability to *understand* the output from the technology for the context in which it is to be *used*.
- (c) Privacy – The discussion of the Code’s fundamental principle of confidentiality is all encompassing and is intended to cover privacy in a principles-based manner. 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). In finalizing the proposals, the IESBA considered that it would be inappropriate to expand on the concept of privacy in the Code given that it gives rise to varying and potentially contradictory approaches to interpretation and application across different jurisdictions.

The IESBA considered and agreed not to include “privacy” as a requirement to be observed by PAs, as might be required under applicable laws or regulations, in the proposed definition of “confidential information” in the Glossary. The IESBA concluded that “privacy” is addressed by national laws and/or regulations which PAs are already required to comply with in the overriding provisions in paragraphs R100.7 to 100.7 A1 of the Code: “...some jurisdictions might have provisions that differ from or go beyond those set out in the Code,” and “accountants in those jurisdictions need to be aware of those differences and comply with the more stringent provisions unless prohibited by law or regulation.”

G. Ethical Leadership

37. The IESBA noted that PAs might be increasingly involved in using, developing or implementing technology. These roles involve dealings with individuals outside the PAs’ employing organizations or firms.
38. Given that ethical behavior is considered to be the cornerstone of public trust, the IESBA is proposing further refinements to emphasize the need for PAs 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” (see proposed revisions in paragraph 120.14 A3).

IV. Significant Matters – Independence (Parts 4A and 4B)

A. Applicability of NAS Provisions When Providing, Selling, Reselling or Licensing Technology (Sections 520 and 600)

39. The survey titled [The Impact of Technology on Auditor Independence](#) indicated that 24% of respondents did not think that NAS provisions are relevant when a firm sells or licenses technology that performs a NAS. Accordingly, the IESBA is proposing revisions 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 (see proposed paragraph 600.6). The proposed guidance is intentionally broad and is intended to encompass 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 its own technology to perform the NAS.
 - Prompt firms to consider the relevance of the NAS provisions in Section 600 when technology is provided, sold, resold¹⁷ or licensed by a firm or a network firm to an audit client (see proposed paragraphs 600.6 and 520.7 A1). That prompt is important to address the fact that 24% of survey respondents did not think that the NAS provisions are relevant when a firm sells or licenses technology that performs a NAS. Therefore, those users of the Code who might look to Section 520 for guidance in such circumstances will be guided by proposed paragraph 520.7 A1 to refer to and consider the provisions in Section 600.
 - Add the concept of “sells” and “resells” to the existing examples of close business relationship where a firm or a network firm distributes or markets the client’s products or services, or vice versa (see proposed revisions in paragraph 520.3 A2 bullet 3).
 - Add an example of a close business relationship arising from arrangements under which a firm or a network firm develops jointly with an audit client, products or solutions that one or both parties sells or licenses to third parties (see proposed paragraph 520.3 A2 bullet 4).

Consideration of Additional Examples

40. The IESBA considered additional examples of close business relationships 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. The IESBA’s current thinking is that at a high level and subject to the details of the selling and licensing arrangements, such arrangements are covered by the second bullet in paragraph 520.3 A2. The IESBA is therefore not proposing the inclusion of such examples.
41. Furthermore, the IESBA considered that if such examples are incorporated, 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. The IESBA is of the view that doing so would detract from the principles-based nature of the Code. For example, an elaboration of the nature of the

¹⁷ The IESBA noted that reselling could consist of a “pass-through” of products developed by third parties to audit clients with no other services attached or could also combine ancillary/ associated services provided by the firm or a network firm with the product being resold. In either case, firms are prompted to consider whether the NAS provisions are relevant to the facts and circumstances of the reselling arrangement.

arrangement (i.e., to determine the closeness of the business relationship) might require the Code to prescribe consideration of a plethora of factors, including but not limited to:

- The promotion of the use of the technology in marketing or proposal materials provided to the end user.
- Whether the technology is in substance the reason why an end user might elect to use a firm for its service delivery.
- Any branding on output created by the technology and delivered to the end user.
- Other considerations, such as fees received or paid in relation to the use of the software from that arrangement.

42. The IESBA is expressly seeking respondents' input on its proposed approach which would not involve providing additional examples of close business relationships in the Code (see paragraphs 40 and 41 above).

B. Factors That Are Relevant in Identifying and Evaluating Threats (Section 600)

43. The proposals include new application material to help in identifying and evaluating the level of threats that might be created by providing technology-related NAS. In particular, the proposals prompt firms to consider their audit clients' dependency on the service being provided, including the frequency with which the service will be provided (see proposed third bullet of paragraph 600.9 A2).

44. The IESBA is of the view that if an audit client requests a firm or a network firm to conduct a service that involves using technology with increased frequency (e.g., due to the insights gained from the application of data analytics), such a service could be regarded as forming part of the audit client's internal controls over financial reporting (i.e., the client's dependency on the NAS). Survey respondents highlighted this scenario as being increasingly relevant in the digital age because the "lines" between management and the firm's responsibilities might become blurred when technology has enabled the provision of frequent or continuous monitoring or analysis.

C. Automated Services and the Placement of "Routine or Mechanical" (Section 400 and Subsection 601)

45. The NAS project clarified 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. Proposed paragraph 601.5 A2 further reminds users of the Code that automated NAS are not necessarily routine or mechanical.

46. In finalizing the technology-related proposals, the IESBA incorporated stakeholder feedback arising from the NAS project which noted that automated services that appear to be "routine or mechanical" could, in substance, result in an assumption of a management responsibility. In this regard, the proposals emphasize that regardless of whether technology is used in performing a professional activity for an audit client, the NAS provisions, including the prohibition on assuming a management responsibility, apply (see proposed paragraph 400.16 A1).

Placement of Material Relating to "Routine or Mechanical" Services

47. Some respondents to the NAS ED questioned the location of the discussion of routine or mechanical services in the Code, and pointed out that such services are not limited to accounting and bookkeeping

or administrative services (see paragraphs 102 and 103 of the [Basis for Conclusions: Revisions to the Non-Assurance Services Provisions of the Code](#)).

48. The IESBA deliberated this matter and came to the view that no change is needed at this time. In coming to this view, the IESBA considered the need to minimize changes to the revised NAS provisions to avoid potentially undermining the revised provisions or adversely impacting their adoption or implementation.

D. IT Systems Services (Subsection 606)

Expanded Description of IT Systems Services

49. The IESBA is proposing an expanded 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 (see proposed paragraph 606.2 A1). The proposal is responsive to survey respondents who expressed support for the Code to include a discussion of IT systems services that involve collecting, storing and hosting of data, and ongoing support, maintenance, and updates of IT systems.
50. The proposed definition of “IT systems services” is intentionally very broad so that the NAS provisions (including the technology-related proposals) could be applicable to the widest range of IT systems services possible. As part of its deliberations, the IESBA considered whether its proposal should include definitions of all the terms used in the expanded description for IT systems services. The IESBA ultimately decided that to do so would be inappropriate because such definitions could have the unintended consequence of narrowing or limiting the application of the proposed changes to only those services clearly falling within such definitions. The IESBA’s intent is to make it explicit that Subsection 606 applies to all IT systems services that might be contemplated for an audit client, rather than limiting it to prescribed descriptions of specific services.

IT Systems Services that Involve Assuming a Management Responsibility for an Audit Client or Might Create a Self-review Threat

51. In developing the proposed revisions to subsection 606 of the Code, the IESBA sought to retain the principles and structure of the revised NAS provisions that were issued in April 2021. The proposed revisions:
- Highlight the types of IT systems services that always involve assuming a management responsibility and are therefore prohibited for all audit clients (see proposed paragraph 606.3 A1). In this regard, the IESBA considered that for such types of IT systems services, 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.
 - Provide examples of IT systems services that might create a self-review threat and are therefore prohibited for PIE audit clients (see proposed paragraph 606.4 A3). In developing the examples, the IESBA also considered whether there are types of IT systems service that always create a self-review threat, and whether there are others that do not usually create a threat.

Services in Relation to the Hosting of an Audit Client’s Data

52. Proposed paragraphs 606.3 A1 and 606.3 A2 expressly deal with hosting of an audit client’s data as a service (either directly on internal servers or indirectly on a cloud provider’s servers). The IESBA determined that providing services in relation to the hosting of an audit client’s data results in the

assumption of a management responsibility. 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.

Providing Advice and Recommendations in Relation to IT Systems

53. The IESBA considered whether the proposals in subsection 606 would preclude firms from providing advice and recommendations in relation to IT systems to their audit clients. The IESBA believes that 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 provide sufficient principles-based guidance.

Withdrawal of the Extant Approach for the Provision of Services Involving the Implementation of Certain “Off-the-shelf” Accounting or Financial Information Reporting Software

54. The IESBA believes that it is no longer appropriate to permit firms to “...implement ‘off-the-shelf’ accounting or financial information reporting software that was not developed by the firm or network firm, if the customization required to meet the client’s needs is not significant...” because the service “...does not usually create a threat...”. Accordingly, the IESBA is proposing to withdraw the related provision in extant subparagraph 606.4 A2(c).
55. In coming to this view, the IESBA noted that the extant provision was intended to address situations where “off-the-shelf” accounting or financial information reporting software comprised retail software packages for direct installation on a desktop computer or laptop, which was common in prior years. Today, “off-the-shelf” software is likely to be licensed directly from the software provider and is typically tailored as part of the implementation process. The IESBA’s current thinking is that implementation of accounting or financial information reporting software might create a self-review threat regardless of materiality and the extent of tailoring (i.e., whether it is customization, configuration, or any other form of implementation).
56. The proposals explain that the “implementation of accounting or financial information reporting software, whether or not it was developed by the firm or a network firm,” might create a self-review threat (see paragraph 606.4 A3). This means that in the case of non-PIE audit clients, firms will need to apply the conceptual framework to address the self-review threat that might be created, whereas for PIE audit clients, the provision of such a service will be prohibited.

E. Proposed Revisions to Part 4B of the Code

57. The proposed revisions preserve the existing alignment between Parts 4A and 4B of the Code (see paragraph 16 above). In particular, the proposed revisions to Part 4B of the Code:
- Indicate by way of an explicit statement that “[Part 4B of the Code] applies to assurance engagements on an entity’s non-financial information, for example, environmental, social and governance (ESG) disclosures” (see proposed revision in paragraph 900.1). This proposal responds to respondents to the technology survey who called for guidance in the Code to cover non-financial reporting. As non-financial reporting is an evolving area, the IESBA took a “light touch” approach to this proposal to keep it specific and narrow, allowing for the possibility of refinements in the future.
 - Provide examples of activities that might involve assuming a management responsibility in relation to the underlying subject matter, and in an attestation engagement, the subject matter information

of an assurance engagement. This includes providing services related to hosting of the underlying subject matter or subject matter information (see proposed paragraphs 900.13 A4 and A5).

- Emphasize that the prohibition on management responsibility applies regardless of the nature and extent of use of technology in performing a professional activity for an assurance client (see proposed paragraph 900.14 A1).
- Provide examples of technology-related arrangements that constitute a close business relationship (see proposed revisions in paragraph 920.3 A2).
- Remind firms of the need to consider and apply Section 950 if a firm provides, sells, resells or licenses technology to an assurance client (see proposed paragraphs 920.6 A1 and 950.5).
- 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 (see proposed revisions in paragraph 950.10 A1).

V. Analysis of Overall Impact of the Proposed Changes

58. The IESBA believes that the proposals are both relevant and important because the use and impact of technology represent one of the most important issues affecting the accountancy profession today and for the foreseeable future. The pace of change in, and use of, technology has accelerated during the COVID-19 pandemic. The proposals include several enhancements to modernize the Code in a principles-based manner with respect to technology.
59. The public interest will be served with these technology-related proposals because they will help ensure that the Code's provisions remain relevant and fit for purpose to respond to the transformative effects of major trends and developments in technology in relation to accounting, assurance and finance functions. Especially in the area of independence, the proposals more clearly delineate the boundaries of technology-related services that are permissible for firms to provide to their audit clients, or technology-related business relationships they might pursue with their audit clients. Such clarification and strengthening of the International Independence Standards will reinforce public trust in the independence of auditors and assurance practitioners.
60. Given the nature and extent of the proposed revisions to the Code, the IESBA believes that some of the proposals will entail costs that may be significant for some stakeholders. In particular, firms can expect some level of implementation costs associated with changes to their internal policies and methodologies, and related awareness and training initiatives. The nature and extent of such costs will depend on the range of services they provide to their clients, especially audit clients. National standard setters and professional accountancy organizations can also expect costs associated with their adoption efforts, including translation where applicable, awareness raising, and education and training initiatives.

VI. Project Timetable and Effective Date

61. The indicative remaining timeline for the Technology project is set out below. This timeline takes into account a 120-day comment period which is intended to provide stakeholders with ample time to understand the proposals in the context of their relevant jurisdictional circumstances and undertake any necessary consultations at their levels or within their networks.

| Indicative Timing | Milestone |
|-----------------------------|---|
| June 20, 2022 | <ul style="list-style-type: none"> • Comment deadline |
| September 2022 | <ul style="list-style-type: none"> • IESBA CAG to provide input on the Task Force's summary of the significant ED comments and its related responses |
| September and December 2022 | <ul style="list-style-type: none"> • IESBA to consider a full review of ED responses and the Task Force's related revisions to the proposed text |
| March 2023 | <ul style="list-style-type: none"> • IESBA CAG to provide final advice for IESBA consideration in finalizing the project • IESBA to approve final technology-related revisions to the Code and determine the effective date |

VII. Guide for Respondents

62. The IESBA welcomes comments on all matters addressed in this ED, but especially on those identified in the Request for Specific Comments below. Comments are most helpful when they refer to specific paragraphs, include the reasons for the comments, and, where appropriate, make specific suggestions for any proposed changes to wording. When a respondent agrees with proposals in this ED, it will be helpful for the IESBA to be made aware of this view.

Request for Specific Comments

63. The IESBA is seeking specific comments on the matters set out below:

Technology-related Considerations When Applying the Conceptual Framework

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

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

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

Consideration of "Complex Circumstances" When Applying the Conceptual Framework

3. Do you support the proposed application material relating to complex circumstances in proposed paragraphs 120.13 A1 to A3?
4. Are you aware of any other considerations, including jurisdiction-specific translation considerations (see paragraph 25 of the explanatory memorandum), that may impact the proposed revisions?

Professional Competence and Due Care

5. Do you support the proposed revisions to explain the skills that PAs need in the digital age, and to enhance transparency in proposed paragraph 113.1 A1 and the proposed revisions to paragraph R113.3, respectively?
6. Do you agree with the IESBA not to include additional new application material (as illustrated in paragraph 29 of the explanatory memorandum) that would make an explicit reference to standards of professional competence such as the IESs (as implemented through the competency requirements in jurisdictions) in the Code?

Confidentiality and Confidential Information

7. Do you support (a) the proposed revisions relating to the description of the fundamental principle of confidentiality in paragraphs 114.1 A1 and 114.1 A3; and (b) the proposed Glossary definition of “confidential information?”
8. Do you agree that “privacy” should not be explicitly included as a requirement to be observed by PAs in the proposed definition of “confidential information” in the Glossary because it is addressed by national laws and regulations which PAs are required to comply with under paragraphs R100.7 to 100.7 A1 of the Code (see sub-paragraph 36(c) of the explanatory memorandum)?

Independence (Parts 4A and 4B)

9. Do you support the proposed revisions to the International Independence Standards, including:
 - (a) The proposed revisions in paragraphs 400.16 A1, 601.5 A2 and A3 relating to “routine or mechanical” services.
 - (b) The additional proposed examples to clarify the technology-related arrangements that constitute a close business relationship in paragraph 520.3 A2. See also paragraphs 40 to 42 of the explanatory memorandum.
 - (c) The proposed revisions to remind PAs providing, selling, reselling or licensing technology to an audit client to apply the NAS provisions in Section 600, including its subsections (see proposed paragraphs 520.7 A1 and 600.6).
10. Do you support the proposed revisions to subsection 606, including:
 - (a) The prohibition on services in relation to hosting (directly or indirectly) of an audit client’s data, and the operation of an audit client’s network security, business continuity and disaster recovery function because they result in the assumption of a management responsibility (see proposed paragraph 606.3 A1 and related paragraph 606.3 A2)?
 - (b) The withdrawal of the presumption in extant subparagraph 606.4 A2(c)¹⁸ and the addition of “Implementing accounting or financial information reporting software, whether or not it

¹⁸ Extant subparagraph 606.4 A2(c) states that “Providing the following IT systems services to an audit client does not usually create a threat as long as individuals within the firm or network firm do not assume a management responsibility: ... Implementing “off-the-shelf” accounting or financial information reporting software that was not developed by the firm or network firm, if the customization required to meet the client’s needs is not significant.”

was developed by the firm or a network firm” as an example of an IT systems service that might create a self-review threat¹⁹ in proposed paragraph 606.4 A3?

- (c) The other examples of IT systems services that might create a self-review threat in proposed paragraph 606.4 A3?

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

Request for General Comments

64. In addition to the request for specific comments above, the IESBA is also seeking comments on the matters set out below:

- *Small- and Medium-sized Entities (SMEs) and Small and Medium Practices (SMPs)* – The IESBA invites comments regarding any aspect of the proposals from SMEs and SMPs.
- *Regulators and Audit Oversight Bodies* – The IESBA invites comments on the proposals from an audit inspection or enforcement perspective from members of the regulatory and audit oversight communities.
- *Developing Nations* – Recognizing that many developing nations have adopted or are in the process of adopting the Code, the IESBA invites respondents from these nations to comment on the proposals, and in particular on any foreseeable difficulties in applying them in their environment.
- *Translations* – Recognizing that many respondents may intend to translate the final changes for adoption in their own environments, the IESBA welcomes comments on potential translation issues respondents may note in reviewing the proposals beyond question 4 in the request for specific comments above.

¹⁹ This means that in the case of non-PIE audit clients, firms will need to apply the conceptual framework to address the threat. For PIE audit clients, the provision of such a service will be prohibited.

**EXPOSURE DRAFT: PROPOSED TECHNOLOGY-RELATED
REVISIONS TO THE CODE
(MARK-UP FROM EXTANT*)**

**PART 1 – COMPLYING WITH THE CODE, FUNDAMENTAL
PRINCIPLES AND CONCEPTUAL FRAMEWORK**

...

SECTION 110 – THE FUNDAMENTAL PRINCIPLES

...

SUBSECTION 113 – PROFESSIONAL COMPETENCE AND DUE CARE

R113.1 A professional accountant shall comply with the principle of professional competence and due care, which requires an accountant to:

- (a) Attain and maintain professional knowledge and skills^s at the level required to ensure that a client or employing organization receives competent professional service, based on current technical and professional standards and relevant legislation; and
- (b) Act diligently and in accordance with applicable technical and professional standards.

113.1 A1 Serving clients and employing organizations with professional competence requires:

- (a) ~~the~~ exercise of sound judgment in applying professional knowledge and skills; and
- (b) The application of interpersonal, communication and organizational skills—when undertaking professional activities.

113.1 A2 Maintaining professional competence requires a continuing awareness and an understanding of relevant technical, professional, business and technology-related developments. Continuing professional development enables a professional accountant to develop and maintain the capabilities to perform competently within the professional environment.

113.1 A3 Diligence encompasses the responsibility to act in accordance with the requirements of an assignment, carefully, thoroughly and on a timely basis.

R113.2 In complying with the principle of professional competence and due care, a professional accountant shall take reasonable steps to ensure that those working in a professional capacity under the accountant's authority have appropriate training and supervision.

* The proposed revisions in this Exposure Draft are to the most recent version of the Code, including revisions that will become effective in December 2022 (i.e., revisions relating to the objectivity of an engagement quality reviewer and other appropriate reviewers, and the revised non-assurance service (NAS) and fee-related provisions of the Code).

This Exposure Draft also takes into account the revisions that the IESBA approved in December 2021 that are subject to approval by the Public Interest Oversight Board (i.e., the quality management-related conforming amendments to the Code, and the revisions relating to the Definitions of Listed Entity and Public Interest Entity).

To access the Code and to obtain final pronouncements issued subsequent to April 2021, visit the IESBA's website at: www.ethicsboard.org/standards-pronouncements.

- R113.3** Where appropriate, a professional accountant shall make clients, the employing organization, or other users of the accountant's professional services or activities, aware of the limitations inherent in the services or activities and provide them with sufficient information to understand the implications of those limitations.

SUBSECTION 114 – CONFIDENTIALITY

- R114.1** A professional accountant shall comply with the principle of confidentiality, which requires an accountant to respect the confidentiality of information acquired as a result of professional and business relationships. An accountant shall:

- (a) Be alert to the possibility of inadvertent disclosure, including in a social environment, and particularly to a close business associate or an immediate or a close family member;
- (b) Maintain confidentiality of information within the firm or employing organization;
- (c) Maintain confidentiality of information disclosed by a prospective client or employing organization;
- (d) Not disclose confidential information acquired as a result of professional and business relationships outside the firm or employing organization without proper and specific authority, unless there is a legal or professional duty or right to disclose;
- (e) Not use confidential information acquired as a result of professional and business relationships for the personal advantage of the accountant or for the advantage of a third party;
- (f) Not use or disclose any confidential information, either acquired or received as a result of a professional or business relationship, after that relationship has ended; and
- (g) Take reasonable steps to ensure that personnel under the accountant's control, and individuals from whom advice and assistance are obtained, respect the accountant's duty of confidentiality.

114.1 A1 Maintaining the confidentiality of information acquired in the course of professional and business relationships involves the professional accountant taking appropriate action to secure such information in the course of its collection, use, transfer, storage, dissemination and lawful destruction.

- 114.1 A²⁴ 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. Nevertheless, the following are circumstances where professional accountants are or might be required to disclose confidential information or when such disclosure might be appropriate:

- (a) Disclosure is required by law, for example:
 - (i) Production of documents or other provision of evidence in the course of legal proceedings; or
 - (ii) Disclosure to the appropriate public authorities of infringements of the law that come to light;
- (b) Disclosure is permitted by law and is authorized by the client or the employing organization; and

- (c) There is a professional duty or right to disclose, when not prohibited by law:
- (i) To comply with the quality review of a professional body;
 - (ii) To respond to an inquiry or investigation by a professional or regulatory body;
 - (iii) To protect the professional interests of a professional accountant in legal proceedings; or
 - (iv) To comply with technical and professional standards, including ethics requirements.

114.1 A³² In deciding whether to disclose 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 consents to the disclosure of information by the professional accountant.
- Whether all the relevant information is known and substantiated, to the extent practicable. Factors affecting the decision to disclose include:
 - Unsubstantiated facts.
 - Incomplete information.
 - Unsubstantiated conclusions.
- The proposed meantype of communicatingen, the information and to whom it is addressed.
- Whether the parties to whom the informationcommunication is to be addressed or access is to be granted are appropriate recipients.

R114.2 A professional accountant shall continue to comply with the principle of confidentiality even after the end of the relationship between the accountant and a client or employing organization. When changing employment or acquiring a new client, the accountant is entitled to use prior experience but shall not use or disclose any confidential information acquired or received as a result of a professional or business relationship.

...

SECTION 120

THE CONCEPTUAL FRAMEWORK

...

Requirements and Application Material

...

Other Considerations when Applying the Conceptual Framework

Bias

120.12 A1 Conscious or unconscious bias affects the exercise of professional judgment when identifying, evaluating and addressing threats to compliance with the fundamental principles.

120.12 A2 Examples of potential bias to be aware of when exercising professional judgment include:

- Anchoring bias, which is a tendency to use an initial piece of information as an anchor against which subsequent information is inadequately assessed.
- Automation bias, which is a tendency to favor output generated from automated systems, even when human reasoning or contradictory information raises questions as to whether such output is reliable or fit for purpose.
- Availability bias, which is a tendency to place more weight on events or experiences that immediately come to mind or are readily available than on those that are not.
- Confirmation bias, which is a tendency to place more weight on information that corroborates an existing belief than information that contradicts or casts doubt on that belief.
- Groupthink, which is a tendency for a group of individuals to discourage individual creativity and responsibility and as a result reach a decision without critical reasoning or consideration of alternatives.
- Overconfidence bias, which is a tendency to overestimate one's own ability to make accurate assessments of risk or other judgments or decisions.
- Representation bias, which is a tendency to base an understanding on a pattern of experiences, events or beliefs that is assumed to be representative.
- Selective perception, which is a tendency for a person's expectations to influence how the person views a particular matter or person.

120.12 A3 Actions that might mitigate the effect of bias include:

- Seeking advice from experts to obtain additional input.
- Consulting with others to ensure appropriate challenge as part of the evaluation process.
- Receiving training related to the identification of bias as part of professional development.

Complex Circumstances

120.13 A1 The circumstances in which professional accountants carry out professional activities vary considerably. Some professional activities might involve complex circumstances that increase the challenges when identifying, evaluating and addressing threats to compliance with the fundamental principles.

120.13 A2 Complex circumstances arise where the relevant facts and circumstances involve:

- (a) Elements that are uncertain; and
- (b) Multiple variables and assumptions.

which are interconnected or interdependent. Such facts and circumstances might also be rapidly changing.

120.13 A3 Managing the evolving interaction of such facts and circumstances as they develop assists the professional accountant to mitigate the challenges arising from complex circumstances. This might include:

- Consulting with others, including experts, to ensure appropriate challenge and additional input as part of the evaluation process.
- Using technology to analyze relevant data to better inform the accountant's judgment.
- Making the firm or employing organization and, if appropriate, relevant stakeholders aware of the inherent uncertainties or difficulties arising from the facts and circumstances.
- Monitoring any developments or changes in the facts and circumstances and assessing whether they might impact any judgments the accountant has made.

Organizational Culture

120.143 A1 The effective application of the conceptual framework by a professional accountant is enhanced when the importance of ethical values that align with the fundamental principles and other provisions set out in the Code is promoted through the internal culture of the accountant's organization.

120.143 A2 The promotion of an ethical culture within an organization is most effective when:

- (a) Leaders and those in managerial roles promote the importance of, and hold themselves and others accountable for demonstrating, the ethical values of the organization;
- (b) Appropriate education and training programs, management processes, and performance evaluation and reward criteria that promote an ethical culture are in place;
- (c) Effective policies and procedures are in place to encourage and protect those who report actual or suspected illegal or unethical behavior, including whistle-blowers; and
- (d) The organization adheres to ethical values in its dealings with third parties.

120.143 A3 Professional accountants are expected to:

- (a) ~~e~~Encourage and promote an ethics-based culture in their organization, taking into account their position and seniority; and
- (b) 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.

...

PART 2 - PROFESSIONAL ACCOUNTANTS IN BUSINESS

SECTION 200

APPLYING THE CONCEPTUAL FRAMEWORK – PROFESSIONAL ACCOUNTANTS IN BUSINESS

...

Requirements and Application Material

General

R200.5 A professional accountant shall comply with the fundamental principles set out in Section 110 and apply the conceptual framework set out in Section 120 to identify, evaluate and address threats to compliance with the fundamental principles.

200.5 A1 A professional accountant has a responsibility to further the legitimate objectives of the accountant's employing organization. The Code does not seek to hinder accountants from fulfilling that responsibility, but addresses circumstances in which compliance with the fundamental principles might be compromised.

200.5 A2 Professional accountants may promote the position of the employing organization when furthering the legitimate goals and objectives of their employing organization, provided that any statements made are neither false nor misleading. Such actions usually would not create an advocacy threat.

200.5 A3 The more senior the position of a professional accountant, the greater will be the ability and opportunity to access information, and to influence policies, decisions made and actions taken by others involved with the employing organization. To the extent that they are able to do so, taking into account their position and seniority in the organization, accountants are expected to encourage and promote an ethics-based culture in the organization in accordance with paragraph 120.143 A3. Examples of actions that might be taken include the introduction, implementation and oversight of:

- Ethics education and training programs.
- Management processes and performance evaluation and reward criteria that promote an ethical culture.
- Ethics and whistle-blowing policies.
- Policies and procedures designed to prevent non-compliance with laws and regulations.

Identifying Threats

200.6 A1 Threats to compliance with the fundamental principles might be created by a broad range of facts and circumstances. The categories of threats are described in paragraph 120.6 A3. The following are examples of facts and circumstances within each of those categories that might create threats for a professional accountant when undertaking a professional activity:

(a) Self-interest Threats

- A professional accountant holding a financial interest in, or receiving a loan or guarantee from, the employing organization.

EXPOSURE DRAFT

- A professional accountant participating in incentive compensation arrangements offered by the employing organization.
 - A professional accountant having access to corporate assets for personal use.
 - A professional accountant being offered a gift or special treatment from a supplier of the employing organization.
- (b) Self-review Threats
- A professional accountant determining the appropriate accounting treatment for a business combination after performing the feasibility study supporting the purchase decision.
- (c) Advocacy Threats
- A professional accountant having the opportunity to manipulate information in a prospectus in order to obtain favorable financing.
- (d) Familiarity Threats
- A professional accountant being responsible for the financial reporting of the employing organization when an immediate or close family member employed by the organization makes decisions that affect the financial reporting of the organization.
 - A professional accountant having a long association with individuals influencing business decisions.
- (e) Intimidation Threats
- A professional accountant or immediate or close family member facing the threat of dismissal or replacement over a disagreement about:
 - o The application of an accounting principle.
 - o The way in which financial information is to be reported.
 - An individual attempting to influence the decision-making process of the professional accountant, for example with regard to the awarding of contracts or the application of an accounting principle.

200.6 A2 The use of technology is a specific circumstance that might create threats to compliance with the fundamental principles. Considerations that are relevant when identifying such threats when a professional accountant relies upon the output from technology include:

- Whether information about how the technology functions is available to the accountant.
- Whether the technology is appropriate for the purpose for which it is to be used.
- Whether the accountant has the professional competence to understand, use and explain the output from the technology.
- Whether the technology incorporates expertise or judgments of the accountant or the employing organization.
- Whether the technology was designed or developed by the accountant or employing organization and therefore might create a self-interest or self-review threat.

...

SECTION 220

PREPARATION AND PRESENTATION OF INFORMATION

...

Requirements and Application Material

...

Relying on the Work of Others or on the Output of Technology

R220.7 A professional accountant who intends to rely on:

- (a) ~~The work of others, individuals, either whether~~ internal or external to the employing organization, or other organizations, or
- (b) The output of technology, whether that technology was developed internally or provided by third parties.

shall exercise professional judgment to determine what steps to take, if any, in order to fulfill the responsibilities set out in paragraph R220.4.

220.7 A1 Factors to consider in determining whether reliance on the work of others is reasonable include:

- The reputation and expertise of, and resources available to, the other individual or organization.
- Whether the other individual is subject to applicable professional and ethics standards.

Such information might be gained from prior association with, or from consulting others about, the other individual or organization.

220.7 A2 Factors to consider in determining whether reliance on the output of technology is reasonable include:

- The nature of the activity to be performed by the technology.
- The expected use of, or extent of reliance on, the output from the technology.
- The professional accountant's ability to understand the output from the technology for the context in which it is to be used.
- Whether the technology is established and effective for the purpose intended.
- Whether new technology has been appropriately tested and evaluated for the purpose intended.
- The reputation of the developer of the technology if acquired from or developed by an external vendor.
- The employing organization's oversight of the design, development, implementation, operation, maintenance, monitoring or updating of the technology.
- The appropriateness of the inputs to the technology, including data and any related decisions.

220.7 A3 Another consideration is whether the professional accountant's position within the employing organization impacts the accountant's ability to obtain information in relation to the factors required to determine whether reliance on the work of others or on the output of technology is reasonable.

...

PART 3 - PROFESSIONAL ACCOUNTANTS IN PUBLIC PRACTICE

SECTION 300

APPLYING THE CONCEPTUAL FRAMEWORK – PROFESSIONAL ACCOUNTANTS IN PUBLIC PRACTICE

...

Requirements and Application Material

General

R300.4 A professional accountant shall comply with the fundamental principles set out in Section 110 and apply the conceptual framework set out in Section 120 to identify, evaluate and address threats to compliance with the fundamental principles.

R300.5 When dealing with an ethics issue, the professional accountant shall consider the context in which the issue has arisen or might arise. Where an individual who is a professional accountant in public practice is performing professional activities pursuant to the accountant's relationship with the firm, whether as a contractor, employee or owner, the individual shall comply with the provisions in Part 2 that apply to these circumstances.

300.5 A1 Examples of situations in which the provisions in Part 2 apply to a professional accountant in public practice include:

- Facing a conflict of interest when being responsible for selecting a vendor for the firm when an immediate family member of the accountant might benefit financially from the contract. The requirements and application material set out in Section 210 apply in these circumstances.
- Preparing or presenting financial information for the accountant's client or firm. The requirements and application material set out in Section 220 apply in these circumstances.
- Being offered an inducement such as being regularly offered complimentary tickets to attend sporting events by a supplier of the firm. The requirements and application material set out in Section 250 apply in these circumstances.
- Facing pressure from an engagement partner to report chargeable hours inaccurately for a client engagement. The requirements and application material set out in Section 270 apply in these circumstances.

Identifying Threats

300.6 A1 Threats to compliance with the fundamental principles might be created by a broad range of facts and circumstances. The categories of threats are described in paragraph 120.6 A3. The following are examples of facts and circumstances within each of those categories of threats

that might create threats for a professional accountant when undertaking a professional service:

(a) Self-interest Threats

- A professional accountant having a direct financial interest in a client.
- A professional accountant quoting a low fee to obtain a new engagement and the fee is so low that it might be difficult to perform the professional service in accordance with applicable technical and professional standards for that price.
- A professional accountant having a close business relationship with a client.
- A professional accountant having access to confidential information that might be used for personal gain.
- A professional accountant discovering a significant error when evaluating the results of a previous professional service performed by a member of the accountant's firm.

(b) Self-review Threats

- A professional accountant issuing an assurance report on the effectiveness of the operation of financial systems after implementing the systems.
- A professional accountant having prepared the original data used to generate records that are the subject matter of the assurance engagement.

(c) Advocacy Threats

- A professional accountant promoting the interests of, or shares in, a client.
- A professional accountant acting as an advocate on behalf of a client in litigation or disputes with third parties.
- A professional accountant lobbying in favor of legislation on behalf of a client.

(d) Familiarity Threats

- A professional accountant having a close or immediate family member who is a director or officer of the client.
- A director or officer of the client, or an employee in a position to exert significant influence over the subject matter of the engagement, having recently served as the engagement partner.
- An audit team member having a long association with the audit client.

(e) Intimidation Threats

- A professional accountant being threatened with dismissal from a client engagement or the firm because of a disagreement about a professional matter.
- A professional accountant feeling pressured to agree with the judgment of a client because the client has more expertise on the matter in question.
- A professional accountant being informed that a planned promotion will not occur unless the accountant agrees with an inappropriate accounting treatment.

- A professional accountant having accepted a significant gift from a client and being threatened that acceptance of this gift will be made public.

300.6 A2 The use of technology is a specific circumstance that might create threats to compliance with the fundamental principles. Considerations that are relevant when identifying such threats when a professional accountant relies upon the output from technology include:

- Whether information about how the technology functions is available to the accountant.
- Whether the technology is appropriate for the purpose for which it is to be used.
- Whether the accountant has the professional competence to understand, use and explain the output from the technology.
- Whether the technology incorporates expertise or judgments of the firm.
- Whether the technology was designed or developed by the firm and therefore might create a self-interest or self-review threat.

...

SECTION 320 PROFESSIONAL APPOINTMENTS

...

Requirements and Application Material

...

Using the Work of an Expert or the Output of Technology

R320.10 When a professional accountant intends to use the work of an expert or the output of technology in the course of undertaking a professional activity, the accountant shall determine whether the use is appropriate for the intended purpose warranted.

320.10 A1 Factors to consider when a professional accountant intends to use the work of an expert include the reputation and expertise of the expert, the resources available to the expert, and the professional and ethics standards applicable to the expert. This information might be gained from prior association with the expert or from consulting others.

320.10 A2 Factors to consider when a professional accountant intends to use the output of technology include:

- The nature of the activity to be performed by the technology.
- The expected use of, or extent of reliance on, the output from the technology.
- The professional accountant's ability to understand the output from the technology for the context in which it is to be used.
- Whether the technology is established and effective for the purpose intended.
- Whether the new technology has been appropriately tested and evaluated for the purpose intended.

- The reputation of the developer of the technology if acquired from or developed by an external vendor.
- The firm's oversight of the design, development, implementation, operation, maintenance, monitoring or updating of the technology.
- The appropriateness of the inputs to the technology, including data and any related decisions.

...

INTERNATIONAL INDEPENDENCE STANDARDS

(PARTS 4A AND 4B)

PART 4A – INDEPENDENCE FOR AUDIT AND REVIEW ENGAGEMENTS

SECTION 400

APPLYING THE CONCEPTUAL FRAMEWORK TO INDEPENDENCE FOR AUDIT AND REVIEW ENGAGEMENTS

...

Requirements and Application Material

...

Prohibition on Assuming Management Responsibilities

R400.15 A firm or a network firm shall not assume a management responsibility for an audit client.

400.15 A1 Management responsibilities involve controlling, leading and directing an entity, including making decisions regarding the acquisition, deployment and control of human, financial, technological, physical and intangible resources.

400.15 A2 When a firm or a network firm assumes a management responsibility for an audit client, self-review, self-interest and familiarity threats are created. Assuming a management responsibility might also create an advocacy threat because the firm or network firm becomes too closely aligned with the views and interests of management.

400.15 A3 Determining whether an activity is a management responsibility depends on the circumstances and requires the exercise of professional judgment. Examples of activities that would be considered a management responsibility include:

- Setting policies and strategic direction.
- Hiring or dismissing employees.
- Directing and taking responsibility for the actions of employees in relation to the employees' work for the entity.
- Authorizing transactions.
- Controlling or managing bank accounts or investments.

- Deciding which recommendations of the firm or network firm or other third parties to implement.
- Reporting to those charged with governance on behalf of management.
- Taking responsibility for:
 - The preparation and fair presentation of the financial statements in accordance with the applicable financial reporting framework.
 - Designing, implementing, monitoring or maintaining internal control.

400.15 A4 Subject to compliance with paragraph R400.16, providing advice and recommendations to assist the management of an audit client in discharging its responsibilities is not assuming a management responsibility. The provision of advice and recommendations to an audit client might create a self-review threat and is addressed in Section 600.

R400.16 When performing a professional activity for an audit client, the firm shall be satisfied that client management makes all judgments and decisions that are the proper responsibility of management. This includes ensuring that the client's management:

- (a) Designates an individual who possesses suitable skill, knowledge and experience to be responsible at all times for the client's decisions and to oversee the activities. Such an individual, preferably within senior management, would understand:
 - (i) The objectives, nature and results of the activities; and
 - (ii) The respective client and firm or network firm responsibilities.

However, the individual is not required to possess the expertise to perform or re-perform the activities.

- (b) Provides oversight of the activities and evaluates the adequacy of the results of the activities performed for the client's purpose.
- (c) Accepts responsibility for the actions, if any, to be taken arising from the results of the activities.

400.16 A1 When technology is used in performing a professional activity for an audit client, the requirements in paragraphs R400.15 and R400.16 apply regardless of the nature or extent of such use.

...

SECTION 520 BUSINESS RELATIONSHIPS

...

Requirements and Application Material

General

520.3 A1 This section contains references to the "materiality" of a financial interest and the "significance" of a business relationship. In determining whether such a financial interest is material to an individual, the combined net worth of the individual and the individual's immediate family members may be taken into account.

520.3 A2 Examples of a close business relationship arising from a commercial relationship or common financial interest include:

- Having a financial interest in a joint venture with either the client or a controlling owner, director or officer or other individual who performs senior managerial activities for that client.
- Arrangements to combine one or more services or products of the firm or a network firm with one or more services or products of the client and to market the package with reference to both parties.
- ~~Distribution or marketing a~~Arrangements under which the firm or a network firm sells, resells, distributes or markets the client's products or services, or the client sells, resells, distributes or markets the firm's or a network firm's products or services.
- Arrangements under which the firm or a network firm develops jointly with the client, products or solutions which one or both parties sell or license to third parties.

...

Buying Goods or Services

520.6 A1 The purchase of goods and services from an audit client by a firm, a network firm, an audit team member, or any of that individual's immediate family does not usually create a threat to independence if the transaction is in the normal course of business and at arm's length. However, such transactions might be of such a nature and magnitude that they create a self-interest threat.

520.6 A2 Examples of actions that might eliminate such a self-interest threat include:

- Eliminating or reducing the magnitude of the transaction.
- Removing the individual from the audit team.

Providing, Selling, Reselling or Licensing Technology

520.7 A1 If a firm or a network firm provides, sells, resells or licenses technology to an audit client, the requirements and application material in Section 600 apply.

...

SECTION 600

PROVISION OF NON-ASSURANCE SERVICES TO AN AUDIT CLIENT

Introduction

600.1 Firms are required to comply with the fundamental principles, be independent, and apply the conceptual framework set out in Section 120 to identify, evaluate and address threats to independence.

600.2 Firms and network firms might provide a range of non-assurance services to their audit clients, consistent with their skills and expertise. Providing non-assurance services to audit clients might create threats to compliance with the fundamental principles and threats to independence.

- 600.3 This section sets out requirements and application material relevant to applying the conceptual framework to identify, evaluate and address threats to independence when providing non-assurance services to audit clients. The subsections that follow set out specific requirements and application material that are relevant when a firm or a network firm provides certain types of non-assurance services to audit clients and indicate the types of threats that might be created as a result.
- 600.4 Some subsections include requirements that expressly prohibit a firm or a network firm from providing certain services to an audit client because the threats created cannot be eliminated and safeguards are not capable of being applied to reduce the threats to an acceptable level.
- 600.5 New business practices, the evolution of financial markets and changes in technology are some developments that make it impossible to draw up an all-inclusive list of non-assurance services that firms and network firms might provide to an audit client. The conceptual framework and the general provisions in this section apply when a firm proposes to a client to provide a non-assurance service for which there are no specific requirements and application material.
- 600.6 The requirements and application material in this section also apply in those circumstances where:
- (a) A firm or a network firm uses technology to provide a non-assurance service to an audit client; or
- (b) A firm or a network firm provides, sells, resells or licenses technology to an audit client.

...

Requirements and Application Material

General

...

Identifying and Evaluating Threats

All Audit Clients

- 600.9 A1 A description of the categories of threats that might arise when a firm or a network firm provides a non-assurance service to an audit client is set out in paragraph 120.6 A3.
- 600.9 A2 Factors that are relevant in identifying the different threats that might be created by providing a non-assurance service to an audit client, and evaluating the level of such threats include:
- The nature, scope, intended use and purpose of the service.
 - The manner in which the service will be provided, such as the personnel to be involved and their location.
 - The client's dependency on the service, including the frequency with which the service will be provided.
 - The legal and regulatory environment in which the service is provided.
 - Whether the client is a public interest entity.

- The level of expertise of the client's management and employees with respect to the type of service provided.
- The extent to which the client determines significant matters of judgment. (Ref: Para. R400.15 to R400.16).
- Whether the outcome of the service will affect the accounting records or matters reflected in the financial statements on which the firm will express an opinion, and, if so:
 - The extent to which the outcome of the service will have a material effect on the financial statements.
 - The degree of subjectivity involved in determining the appropriate amounts or treatment for those matters reflected in the financial statements.
- The nature and extent of the impact of the service, if any, on the systems that generate information that forms a significant part of the client's:
 - Accounting records or financial statements on which the firm will express an opinion.
 - Internal controls over financial reporting.
- The degree of reliance that will be placed on the outcome of the service as part of the audit.
- The fee relating to the provision of the non-assurance service.

600.9 A3 Subsections 601 to 610 include examples of additional factors that are relevant in identifying threats to independence created by providing certain non-assurance services, and evaluating the level of such threats.

...

Self-review threats

600.13 A1 When a firm or a network firm provides a non-assurance service to an audit client, there might be a risk of the firm auditing its own or the network firm's work, thereby giving rise to a self-review threat. A self-review threat is the threat that a firm or a network firm will not appropriately evaluate the results of a previous judgment made or an activity performed by an individual within the firm or network firm as part of a non-assurance service on which the audit team will rely when forming a judgment as part of an audit.

R600.14 Before providing a non-assurance service to an audit client, a firm or a network firm shall determine whether the provision of that service might create a self-review threat by evaluating whether there is a risk that:

- (a) The results of the service will form part of or affect the accounting records, the internal controls over financial reporting, or the financial statements on which the firm will express an opinion; and
- (b) In the course of the audit of those financial statements on which the firm will express an opinion, the audit team will evaluate or rely on any judgments made or activities performed by the firm or network firm when providing the service.

Audit Clients that are Public Interest Entities

600.15 A1 When the audit client is a public interest entity, stakeholders have heightened expectations regarding the firm's independence. These heightened expectations are relevant to the reasonable and informed third party test used to evaluate a self-review threat created by providing a non-assurance service to an audit client that is a public interest entity.

600.15 A2 Where the provision of a non-assurance service to an audit client that is a public interest entity creates a self-review threat, that threat cannot be eliminated, and safeguards are not capable of being applied to reduce that threat to an acceptable level.

Self-review threats

R600.16 A firm or a network firm shall not provide a non-assurance service to an audit client that is a public interest entity if the provision of that service might create a self-review threat in relation to the audit of the financial statements on which the firm will express an opinion. (Ref: Para. 600.13 A1 and R600.14).

...

SUBSECTION 601 – ACCOUNTING AND BOOKKEEPING SERVICES

Introduction

601.1 In addition to the specific requirements and application material in this subsection, the requirements and application material in paragraphs 600.1 to 600.27 A1 are relevant to applying the conceptual framework when providing accounting and bookkeeping services to an audit client.

...

Requirements and Application Material

...

Audit Clients that are Not Public Interest Entities

R601.5 A firm or a network firm shall not provide to an audit client that is not a public interest entity accounting and bookkeeping services, including preparing financial statements on which the firm will express an opinion or financial information which forms the basis of such financial statements, unless:

- (a) The services are of a routine or mechanical nature; and
- (b) The firm addresses any threats that are not at an acceptable level.

601.5 A1 Accounting and bookkeeping services that are routine or mechanical:

- (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 judgment.

601.5 A2 Accounting and bookkeeping services can either be manual or automated. In determining whether an automated service is routine or mechanical, factors to be considered include how

the technology functions and whether the technology is based on expertise or judgments of the firm or a network firm.

601.5 A³² Examples of services, whether manual or automated, that might be regarded as routine or mechanical include:

- Preparing payroll calculations or reports based on client-originated data for approval and payment by the client.
- Recording recurring transactions for which amounts are easily determinable from source documents or originating data, such as a utility bill where the client has determined or approved the appropriate account classification.
- Calculating depreciation on fixed assets when the client determines the accounting policy and estimates of useful life and residual values.
- Posting transactions coded by the client to the general ledger.
- Posting client-approved entries to the trial balance.
- Preparing financial statements based on information in the client-approved trial balance and preparing related notes based on client-approved records.

The firm or a network firm may provide such services to audit clients that are not public interest entities provided that the firm or network firm complies with the requirements of paragraph R400.16 to ensure that it does not assume a management responsibility in connection with the service and with the requirement in paragraph R601.5 (b).

601.5 A⁴³ Examples of actions that might be safeguards to address a self-review threat created when providing accounting and bookkeeping services of a routine or mechanical nature to an audit client that is not a public interest entity include:

- Using professionals who are not audit team members to perform the service.
- Having an appropriate reviewer who was not involved in providing the service review the audit work or service performed.

...

SUBSECTION 606 – INFORMATION TECHNOLOGY SYSTEMS SERVICES

Introduction

606.1 In addition to the specific requirements and application material in this subsection, the requirements and application material in paragraphs 600.1 to 600.27 A1 are relevant to applying the conceptual framework when providing an information technology (IT) systems service to an audit client.

Requirements and Application Material

Description of Service

606.2 A1 IT systems services comprise a broad range of services including:

- Designing or developing hardware or software IT systems.

- Implementing IT systems, including installation, configuration, interfacing, or customization.
- Operating, maintaining, monitoring, or updating IT systems.
- Collecting or storing data or managing (directly or indirectly) the hosting of data on behalf of the audit client.

606.2 A~~2~~¹ ~~Services related to IT systems include the design or implementation of hardware or software systems.~~The IT systems might:

- (a) Aggregate source data;
- (b) Form part of the internal control over financial reporting; or
- (c) Generate information that affects the accounting records or financial statements, including related disclosures.

However, the IT systems might also involve matters that are unrelated to the audit client's accounting records or the internal control over financial reporting or financial statements.

Risk of Assuming Management Responsibility When Providing an IT Systems Service

R606.3 Paragraph R400.15 precludes a firm or a network firm from assuming a management responsibility. When providing IT systems services to an audit client, the firm or network firm shall be satisfied that:

- (a) The client acknowledges its responsibility for establishing and monitoring a system of internal controls;
- ~~(b) The client assigns the responsibility to make all management decisions with respect to the design and implementation of the hardware or software system to a competent employee, preferably within senior management;~~
- ~~(c)~~ (b) The client, through a competent individual, preferably within senior management, makes all management decisions that are the proper responsibility of management with respect to the design, development, and implementation, operation, maintenance, monitoring, or updating of the IT systems process;
- ~~(d)~~ (c) The client evaluates the adequacy and results of the design, development, and implementation, operation, maintenance, monitoring, or updating of the IT system; and
- ~~(e)~~ (d) The client is responsible for operating the IT system ~~(hardware or software)~~ and for the data it generates and uses ~~or generates~~.

606.3 A1 Examples of IT systems services that result in the assumption of a management responsibility include where a firm or a network firm:

- Provides services in relation to the hosting (directly or indirectly) of an audit client's data.
- Operates an audit client's network security, business continuity or disaster recovery function.

606.3 A2 The collection, receipt and retention of data provided by an audit client to enable the provision of a permissible service to that client does not result in an assumption of management responsibility.

Potential Threats Arising from the Provision of IT Systems Services

All Audit Clients

606.4 A1 Providing IT systems services to an audit client might create a self-review threat when there is a risk that the results of the services will affect the audit of the financial statements on which the firm will express an opinion.

~~606.4 A2 Providing the following IT systems services to an audit client does not usually create a threat as long as individuals within the firm or network firm do not assume a management responsibility:~~

- ~~(a) Designing or implementing IT systems that are unrelated to internal control over financial reporting;~~
- ~~(b) Designing or implementing IT systems that do not generate information forming part of the accounting records or financial statements; and~~
- ~~(c) Implementing “off-the-shelf” accounting or financial information reporting software that was not developed by the firm or network firm, if the customization required to meet the client’s needs is not significant.~~

606.4 A²³ Factors that are relevant in identifying a self-review threat created by providing an IT systems service to an audit client, and evaluating the level of such a threat include:

- The nature of the service.
- The nature of the client’s IT systems and the extent to which the IT systems service impacts or interacts with the client’s accounting records, internal controls over financial reporting or financial statements.
- The degree of reliance that will be placed on the particular IT systems as part of the audit.

When a self-review threat for an audit client that is a public interest entity has been identified, paragraph R606.6 applies.

~~606.4 A3 Examples of IT systems services that might create a self-review threat when they form part of or affect an audit client’s accounting records or system of internal control over financial reporting include:~~

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

Audit Clients that are Not Public Interest Entities

606.5 A1 An example of an action that might be a safeguard to address a self-review threat created by the provision of an IT systems service to an audit client that is not a public interest entity is using professionals who are not audit team members to perform the service.

Audit Clients that are Public Interest Entities

R606.6 A firm or a network firm shall not provide IT systems services to an audit client that is a public interest entity if the provision of such services might create a self-review threat (Ref: Para. R600.14 and R600.16).

~~606.6 A1—Examples of services that are prohibited because they give rise to a self-review threat include those involving designing or implementing IT systems that:~~

- ~~• Form part of the internal control over financial reporting; or~~
- ~~• Generate information for the client's accounting records or financial statements on which the firm will express an opinion.~~

...

PART 4B – INDEPENDENCE FOR ASSURANCE ENGAGEMENTS OTHER THAN AUDIT AND -REVIEW ENGAGEMENTS

SECTION 900

APPLYING THE CONCEPTUAL FRAMEWORK TO INDEPENDENCE FOR ASSURANCE ENGAGEMENTS OTHER THAN AUDIT AND REVIEW ENGAGEMENTS

Introduction

General

900.1 This Part applies to assurance engagements other than audit engagements and review engagements. Examples of such engagements include:

- Assurance on an entity's key performance indicators.
- Assurance on an entity's compliance with law or regulation.
- Assurance on performance criteria, such as value for money, achieved by a public sector body.
- Assurance on the effectiveness of an entity's system of internal control.
- Assurance on an entity's non-financial information, for example, environmental, social and governance disclosures, including greenhouse gas statements.
- An audit of specific elements, accounts or items of a financial statement.

...

Requirements and Application Material

...

Prohibition on Assuming Management Responsibilities

R900.13 A firm shall not assume a management responsibility related to the underlying subject matter and, in an attestation engagement, the subject matter information of an assurance engagement provided by the firm. If the firm assumes a management responsibility as part of any other service provided to the assurance client, the firm shall ensure that the responsibility is not

- related to the underlying subject matter and, in an attestation engagement, the subject matter information of the assurance engagement provided by the firm.
- 900.13 A1 Management responsibilities involve controlling, leading and directing an entity, including making decisions regarding the acquisition, deployment and control of human, financial, technological, physical and intangible resources.
- 900.13 A2 When a firm assumes a management responsibility related to the underlying subject matter and, in an attestation engagement, the subject matter information of an assurance engagement, self-review, self-interest and familiarity threats are created. Assuming a management responsibility might create an advocacy threat because the firm becomes too closely aligned with the views and interests of management.
- 900.13 A3 Determining whether an activity is a management responsibility depends on the circumstances and requires the exercise of professional judgment. Examples of activities that would be considered a management responsibility include:
- Setting policies and strategic direction.
 - Hiring or dismissing employees.
 - Directing and taking responsibility for the actions of employees in relation to the employees' work for the entity.
 - Authorizing transactions.
 - Controlling or managing bank accounts or investments.
 - Deciding which recommendations of the firm or other third parties to implement.
 - Reporting to those charged with governance on behalf of management.
 - Taking responsibility for designing, implementing, monitoring and maintaining internal control.
- 900.13 A4 Examples of assuming a management responsibility in relation to the underlying subject matter and, in an attestation engagement, the subject matter information of an assurance engagement, include:
- Providing services in relation to the hosting (directly or indirectly) of the underlying subject matter or subject matter information.
 - Operating an assurance client's network security, business continuity or disaster recovery function related to the underlying subject matter or subject matter information.
- 900.13 A5 The collection, receipt and retention of data to enable the performance of assurance and non-assurance engagements does not result in an assumption of management responsibility.
- 900.13 A⁶ Subject to compliance with paragraph R900.14, providing advice and recommendations to assist the management of an assurance client in discharging its responsibilities is not assuming a management responsibility.
- R900.14** When performing a professional activity for an assurance client that is related to the underlying subject matter and, in an attestation engagement, the subject matter information of the assurance engagement, the firm shall be satisfied that client management makes all related

judgments and decisions that are the proper responsibility of management. This includes ensuring that the client's management:

- (a) Designates an individual who possesses suitable skill, knowledge and experience to be responsible at all times for the client's decisions and to oversee the activities. Such an individual, preferably within senior management, would understand:
 - (i) The objectives, nature and results of the activities; and
 - (ii) The respective client and firm responsibilities.

However, the individual is not required to possess the expertise to perform or re-perform the activities.

- (b) Provides oversight of the activities and evaluates the adequacy of the results of the activity performed for the client's purpose; and
- (c) Accepts responsibility for the actions, if any, to be taken arising from the results of the activities.

900.14 A1 When technology is used in performing a professional activity for an assurance client, the requirements in paragraphs R900.13 and R900.14 apply regardless of the nature or extent of such use.

...

SECTION 920 BUSINESS RELATIONSHIPS

...

Requirements and Application Material

General

- 920.3 A1 This section contains references to the "materiality" of a financial interest and the "significance" of a business relationship. In determining whether such a financial interest is material to an individual, the combined net worth of the individual and the individual's immediate family members may be taken into account.
- 920.3 A2 Examples of a close business relationship arising from a commercial relationship or common financial interest include:
 - Having a financial interest in a joint venture with either the assurance client or a controlling owner, director or officer or other individual who performs senior managerial activities for that client.
 - Arrangements to combine one or more services or products of the firm with one or more services or products of the client and to market the package with reference to both parties.
 - ~~Distribution or marketing a~~Arrangements under which the firm sells, resells, distributes or markets the client's products or services, or the client sells, resells, distributes or markets the firm's products or services.

- Arrangements under which a firm develops jointly with the assurance client, products or solutions which one or both parties sell or license to third parties.

...

Buying Goods or Services

920.5 A1 The purchase of goods and services from an assurance client by a firm, or an assurance team member, or any of that individual's immediate family does not usually create a threat to independence if the transaction is in the normal course of business and at arm's length. However, such transactions might be of such a nature and magnitude that they create a self-interest threat.

920.5 A2 Examples of actions that might eliminate such a self-interest threat include:

- Eliminating or reducing the magnitude of the transaction.
- Removing the individual from the assurance team.

Providing, Selling, Reselling or Licensing Technology

920.6 A1 If a firm provides, sells, resells or licenses technology to an assurance client, the requirements and application material in Section 950 apply.

...

SECTION 950

PROVISION OF NON-ASSURANCE SERVICES TO ASSURANCE CLIENTS

...

Introduction

950.1 Firms are required to comply with the fundamental principles, be independent, and apply the conceptual framework set out in Section 120 to identify, evaluate and address threats to independence.

950.2 Firms might provide a range of non-assurance services to their assurance clients, consistent with their skills and expertise. Providing certain non-assurance services to assurance clients might create threats to compliance with the fundamental principles and threats to independence.

950.3 This section sets out requirements and application material relevant to applying the conceptual framework to identify, evaluate and address threats to independence when providing non-assurance services to assurance clients.

950.4 New business practices, the evolution of financial markets and changes in technology are some developments that make it impossible to draw up an all-inclusive list of non-assurance services that firms might provide to an assurance client. The conceptual framework and the general

provisions in this section apply when a firm proposes to a client to provide a non- assurance service for which there are no specific requirements and application material.

950.5 The requirements and application material in this section also apply in those circumstances where:

- (a) A firm uses technology to provide a non-assurance service to an assurance client; or
- (b) A firm provides, sells, resells or licenses technology to an assurance client.

Requirements and Application Material

General

...

Identifying and Evaluating Threats

950.7 A1 A description of the categories of threats that might arise when a firm provides a non-assurance service to an assurance client is set out in paragraph 120.6 A3.

950.7 A2 Factors that are relevant in identifying and evaluating the different threats that might be created by providing a non-assurance service to an assurance client include:

- The nature, scope, intended use and purpose of the service.
- The manner in which the service will be provided, such as the personnel to be involved and their location.
- The client's dependency on the service, including the frequency with which the service will be provided.
- The legal and regulatory environment in which the service is provided.
- Whether the client is a public interest entity.
- The level of expertise of the client's management and employees with respect to the type of service provided.
- Whether the outcome of the service will affect the underlying subject matter and, in an attestation engagement, matters reflected in the subject matter information of the assurance engagement, and, if so:
 - The extent to which the outcome of the service will have a material effect on the underlying subject matter and, in an attestation engagement, the subject matter information of the assurance engagement.
 - The extent to which the assurance client determines significant matters of judgment (Ref: Para. R900.13 to R900.14).
- The degree of reliance that will be placed on the outcome of the service as part of the assurance engagement.
- The fee relating to the provision of the non-assurance service.

...

Self-Review Threats

950.10 A1 A self-review threat might be created if, in an attestation engagement, the firm is involved in the preparation of subject matter information which subsequently becomes the subject matter information of an assurance engagement. Examples of non-assurance services that might create such self-review threats when providing services related to the subject matter information of an assurance engagement include:

- (a) Developing and preparing prospective information and subsequently issuing an assurance report on this information.
- (b) Performing a valuation that is related to or forms part of the subject matter information of an assurance engagement.

(c) 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.

Assurance clients that are public interest entities

950.11 A1 Expectations about a firm's independence are heightened when an assurance engagement is undertaken by a firm for a public interest entity and the results of that engagement will be:

- (a) Made available publicly, including to shareholders and other stakeholders; or
- (b) Provided to an entity or organization established by law or regulation to oversee the operation of a business sector or activity.

Consideration of these expectations forms part of the reasonable and informed third party test applied when determining whether to provide a non-assurance service to an assurance client.

950.11 A2 If a self-review threat exists in relation to an engagement undertaken in the circumstances described in paragraph 950.11 A1 (b), the firm is encouraged to disclose the existence of that self-review threat and the steps taken to address it to the party engaging the firm or those charged with governance of the assurance client and to the entity or organization established by law or regulation to oversee the operation of a business sector or activity to which the results of the engagement will be provided.

...

GLOSSARY, INCLUDING LISTS OF ABBREVIATIONS

...

Conceptual framework This term is described in Section 120.

Confidential information Any information, data or other material in whatever form or medium (including written, electronic, visual or oral) that is not in the public domain.

Contingent fee A fee calculated on a predetermined basis relating to the outcome of a transaction or the result of the services performed by the firm. A fee that is established by a court or other public authority is not a contingent fee.

**EXPOSURE DRAFT: PROPOSED TECHNOLOGY-RELATED
REVISIONS TO THE CODE
(CLEAN)**

**PART 1 – COMPLYING WITH THE CODE, FUNDAMENTAL
PRINCIPLES AND CONCEPTUAL FRAMEWORK**

...

SECTION 110 – THE FUNDAMENTAL PRINCIPLES

...

SUBSECTION 113 – PROFESSIONAL COMPETENCE AND DUE CARE

- R113.1** A professional accountant shall comply with the principle of professional competence and due care, which requires an accountant to:
- (a)** Attain and maintain professional knowledge and skills at the level required to ensure that a client or employing organization receives competent professional service, based on current technical and professional standards and relevant legislation; and
 - (b)** Act diligently and in accordance with applicable technical and professional standards.
- 113.1 A1 Serving clients and employing organizations with professional competence requires:
- (a)** The exercise of sound judgment in applying professional knowledge and skills; and
 - (b)** The application of interpersonal, communication and organizational skills.
- 113.1 A2 Maintaining professional competence requires a continuing awareness and an understanding of relevant technical, professional, business and technology-related developments. Continuing professional development enables a professional accountant to develop and maintain the capabilities to perform competently within the professional environment.
- 113.1 A3 Diligence encompasses the responsibility to act in accordance with the requirements of an assignment, carefully, thoroughly and on a timely basis.
- R113.2** In complying with the principle of professional competence and due care, a professional accountant shall take reasonable steps to ensure that those working in a professional capacity under the accountant's authority have appropriate training and supervision.
- R113.3** Where appropriate, a professional accountant shall make clients, the employing organization, or other users of the accountant's professional services or activities, aware of the limitations inherent in the services or activities and provide them with sufficient information to understand the implications of those limitations.

SUBSECTION 114 – CONFIDENTIALITY

R114.1 A professional accountant shall comply with the principle of confidentiality, which requires an accountant to respect the confidentiality of information acquired as a result of professional and business relationships. An accountant shall:

- (a) Be alert to the possibility of inadvertent disclosure, including in a social environment, and particularly to a close business associate or an immediate or a close family member;
- (b) Maintain confidentiality of information within the firm or employing organization;
- (c) Maintain confidentiality of information disclosed by a prospective client or employing organization;
- (d) Not disclose confidential information acquired as a result of professional and business relationships outside the firm or employing organization without proper and specific authority, unless there is a legal or professional duty or right to disclose;
- (e) Not use confidential information acquired as a result of professional and business relationships for the personal advantage of the accountant or for the advantage of a third party;
- (f) Not use or disclose any confidential information, either acquired or received as a result of a professional or business relationship, after that relationship has ended; and
- (g) Take reasonable steps to ensure that personnel under the accountant's control, and individuals from whom advice and assistance are obtained, respect the accountant's duty of confidentiality.

114.1 A1 Maintaining the confidentiality of information acquired in the course of professional and business relationships involves the professional accountant taking appropriate action to secure such information in the course of its collection, use, transfer, storage, dissemination and lawful destruction.

114.1 A2 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. Nevertheless, the following are circumstances where professional accountants are or might be required to disclose confidential information or when such disclosure might be appropriate:

- (a) Disclosure is required by law, for example:
 - (i) Production of documents or other provision of evidence in the course of legal proceedings; or
 - (ii) Disclosure to the appropriate public authorities of infringements of the law that come to light;
- (b) Disclosure is permitted by law and is authorized by the client or the employing organization; and
- (c) There is a professional duty or right to disclose, when not prohibited by law:
 - (i) To comply with the quality review of a professional body;
 - (ii) To respond to an inquiry or investigation by a professional or regulatory body;

- (iii) To protect the professional interests of a professional accountant in legal proceedings; or
- (iv) To comply with technical and professional standards, including ethics requirements.

114.1 A3 In deciding whether to disclose 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 consents to the disclosure of information by the professional accountant.
- Whether all the relevant information is known and substantiated, to the extent practicable. Factors affecting the decision to disclose include:
 - Unsubstantiated facts.
 - Incomplete information.
 - Unsubstantiated conclusions.
- The proposed means of communicating, the information.
- Whether the parties to whom the information is to be addressed or access is to be granted are appropriate recipients.

R114.2 A professional accountant shall continue to comply with the principle of confidentiality even after the end of the relationship between the accountant and a client or employing organization. When changing employment or acquiring a new client, the accountant is entitled to use prior experience but shall not use or disclose any confidential information acquired or received as a result of a professional or business relationship.

...

SECTION 120

THE CONCEPTUAL FRAMEWORK

...

Requirements and Application Material

...

Other Considerations when Applying the Conceptual Framework

Bias

- 120.12 A1 Conscious or unconscious bias affects the exercise of professional judgment when identifying, evaluating and addressing threats to compliance with the fundamental principles.
- 120.12 A2 Examples of potential bias to be aware of when exercising professional judgment include:
- Anchoring bias, which is a tendency to use an initial piece of information as an anchor against which subsequent information is inadequately assessed.

- Automation bias, which is a tendency to favor output generated from automated systems, even when human reasoning or contradictory information raises questions as to whether such output is reliable or fit for purpose.
- Availability bias, which is a tendency to place more weight on events or experiences that immediately come to mind or are readily available than on those that are not.
- Confirmation bias, which is a tendency to place more weight on information that corroborates an existing belief than information that contradicts or casts doubt on that belief.
- Groupthink, which is a tendency for a group of individuals to discourage individual creativity and responsibility and as a result reach a decision without critical reasoning or consideration of alternatives.
- Overconfidence bias, which is a tendency to overestimate one's own ability to make accurate assessments of risk or other judgments or decisions.
- Representation bias, which is a tendency to base an understanding on a pattern of experiences, events or beliefs that is assumed to be representative.
- Selective perception, which is a tendency for a person's expectations to influence how the person views a particular matter or person.

120.12 A3 Actions that might mitigate the effect of bias include:

- Seeking advice from experts to obtain additional input.
- Consulting with others to ensure appropriate challenge as part of the evaluation process.
- Receiving training related to the identification of bias as part of professional development.

Complex Circumstances

120.13 A1 The circumstances in which professional accountants carry out professional activities vary considerably. Some professional activities might involve complex circumstances that increase the challenges when identifying, evaluating and addressing threats to compliance with the fundamental principles.

120.13 A2 Complex circumstances arise where the relevant facts and circumstances involve:

- (a) Elements that are uncertain; and
- (b) Multiple variables and assumptions,

which are interconnected or interdependent. Such facts and circumstances might also be rapidly changing.

120.13 A3 Managing the evolving interaction of such facts and circumstances as they develop assists the professional accountant to mitigate the challenges arising from complex circumstances. This might include:

- Consulting with others, including experts, to ensure appropriate challenge and additional input as part of the evaluation process.
- Using technology to analyze relevant data to better inform the accountant's judgment.

- Making the firm or employing organization and, if appropriate, relevant stakeholders aware of the inherent uncertainties or difficulties arising from the facts and circumstances.
- Monitoring any developments or changes in the facts and circumstances and assessing whether they might impact any judgments the accountant has made.

Organizational Culture

120.14 A1 The effective application of the conceptual framework by a professional accountant is enhanced when the importance of ethical values that align with the fundamental principles and other provisions set out in the Code is promoted through the internal culture of the accountant's organization.

120.14 A2 The promotion of an ethical culture within an organization is most effective when:

- (a) Leaders and those in managerial roles promote the importance of, and hold themselves and others accountable for demonstrating, the ethical values of the organization;
- (b) Appropriate education and training programs, management processes, and performance evaluation and reward criteria that promote an ethical culture are in place;
- (c) Effective policies and procedures are in place to encourage and protect those who report actual or suspected illegal or unethical behavior, including whistle-blowers; and
- (d) The organization adheres to ethical values in its dealings with third parties.

120.14 A3 Professional accountants are expected to:

- (a) Encourage and promote an ethics-based culture in their organization, taking into account their position and seniority; and
- (b) 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.

...

PART 2 - PROFESSIONAL ACCOUNTANTS IN BUSINESS

SECTION 200

APPLYING THE CONCEPTUAL FRAMEWORK – PROFESSIONAL ACCOUNTANTS IN BUSINESS

...

Requirements and Application Material

General

R200.5 A professional accountant shall comply with the fundamental principles set out in Section 110 and apply the conceptual framework set out in Section 120 to identify, evaluate and address threats to compliance with the fundamental principles.

200.5 A1 A professional accountant has a responsibility to further the legitimate objectives of the accountant's employing organization. The Code does not seek to hinder accountants from

fulfilling that responsibility, but addresses circumstances in which compliance with the fundamental principles might be compromised.

- 200.5 A2 Professional accountants may promote the position of the employing organization when furthering the legitimate goals and objectives of their employing organization, provided that any statements made are neither false nor misleading. Such actions usually would not create an advocacy threat.
- 200.5 A3 The more senior the position of a professional accountant, the greater will be the ability and opportunity to access information, and to influence policies, decisions made and actions taken by others involved with the employing organization. To the extent that they are able to do so, taking into account their position and seniority in the organization, accountants are expected to encourage and promote an ethics-based culture in the organization in accordance with paragraph 120.14 A3. Examples of actions that might be taken include the introduction, implementation and oversight of:
- Ethics education and training programs.
 - Management processes and performance evaluation and reward criteria that promote an ethical culture.
 - Ethics and whistle-blowing policies.
 - Policies and procedures designed to prevent non-compliance with laws and regulations.

Identifying Threats

200.6 A1 Threats to compliance with the fundamental principles might be created by a broad range of facts and circumstances. The categories of threats are described in paragraph 120.6 A3. The following are examples of facts and circumstances within each of those categories that might create threats for a professional accountant when undertaking a professional activity:

- (a) Self-interest Threats
- A professional accountant holding a financial interest in, or receiving a loan or guarantee from, the employing organization.
 - A professional accountant participating in incentive compensation arrangements offered by the employing organization.
 - A professional accountant having access to corporate assets for personal use.
 - A professional accountant being offered a gift or special treatment from a supplier of the employing organization.
- (b) Self-review Threats
- A professional accountant determining the appropriate accounting treatment for a business combination after performing the feasibility study supporting the purchase decision.
- (c) Advocacy Threats
- A professional accountant having the opportunity to manipulate information in a prospectus in order to obtain favorable financing.
- (d) Familiarity Threats

EXPOSURE DRAFT

- A professional accountant being responsible for the financial reporting of the employing organization when an immediate or close family member employed by the organization makes decisions that affect the financial reporting of the organization.
- A professional accountant having a long association with individuals influencing business decisions.

(e) Intimidation Threats

- A professional accountant or immediate or close family member facing the threat of dismissal or replacement over a disagreement about:
 - o The application of an accounting principle.
 - o The way in which financial information is to be reported.
- An individual attempting to influence the decision-making process of the professional accountant, for example with regard to the awarding of contracts or the application of an accounting principle.

200.6 A2 The use of technology is a specific circumstance that might create threats to compliance with the fundamental principles. Considerations that are relevant when identifying such threats when a professional accountant relies upon the output from technology include:

- Whether information about how the technology functions is available to the accountant.
- Whether the technology is appropriate for the purpose for which it is to be used.
- Whether the accountant has the professional competence to understand, use and explain the output from the technology.
- Whether the technology incorporates expertise or judgments of the accountant or the employing organization.
- Whether the technology was designed or developed by the accountant or employing organization and therefore might create a self-interest or self-review threat.

...

SECTION 220

PREPARATION AND PRESENTATION OF INFORMATION

...

Requirements and Application Material

...

Relying on the Work of Others or on the Output of Technology

R220.7 A professional accountant who intends to rely on:

- (a) The work of others, whether internal or external to the employing organization, or other organizations, or
- (b) The output of technology, whether that technology was developed internally or provided by third parties,

shall exercise professional judgment to determine what steps to take, if any, in order to fulfill the responsibilities set out in paragraph R220.4.

220.7 A1 Factors to consider in determining whether reliance on the work of others is reasonable include:

- The reputation and expertise of, and resources available to, the other individual or organization.
- Whether the other individual is subject to applicable professional and ethics standards.

Such information might be gained from prior association with, or from consulting others about, the other individual or organization.

220.7 A2 Factors to consider in determining whether reliance on the output of technology is reasonable include:

- The nature of the activity to be performed by the technology.
- The expected use of, or extent of reliance on, the output from the technology.
- The professional accountant's ability to understand the output from the technology for the context in which it is to be used.
- Whether the technology is established and effective for the purpose intended.
- Whether new technology has been appropriately tested and evaluated for the purpose intended.
- The reputation of the developer of the technology if acquired from or developed by an external vendor.
- The employing organization's oversight of the design, development, implementation, operation, maintenance, monitoring or updating of the technology.
- The appropriateness of the inputs to the technology, including data and any related decisions.

220.7 A3 Another consideration is whether the professional accountant's position within the employing organization impacts the accountant's ability to obtain information in relation to the factors

required to determine whether reliance on the work of others or on the output of technology is reasonable.

...

PART 3 - PROFESSIONAL ACCOUNTANTS IN PUBLIC PRACTICE

SECTION 300

APPLYING THE CONCEPTUAL FRAMEWORK – PROFESSIONAL ACCOUNTANTS IN PUBLIC PRACTICE

...

Requirements and Application Material

General

R300.4 A professional accountant shall comply with the fundamental principles set out in Section 110 and apply the conceptual framework set out in Section 120 to identify, evaluate and address threats to compliance with the fundamental principles.

R300.5 When dealing with an ethics issue, the professional accountant shall consider the context in which the issue has arisen or might arise. Where an individual who is a professional accountant in public practice is performing professional activities pursuant to the accountant's relationship with the firm, whether as a contractor, employee or owner, the individual shall comply with the provisions in Part 2 that apply to these circumstances.

300.5 A1 Examples of situations in which the provisions in Part 2 apply to a professional accountant in public practice include:

- Facing a conflict of interest when being responsible for selecting a vendor for the firm when an immediate family member of the accountant might benefit financially from the contract. The requirements and application material set out in Section 210 apply in these circumstances.
- Preparing or presenting financial information for the accountant's client or firm. The requirements and application material set out in Section 220 apply in these circumstances.
- Being offered an inducement such as being regularly offered complimentary tickets to attend sporting events by a supplier of the firm. The requirements and application material set out in Section 250 apply in these circumstances.
- Facing pressure from an engagement partner to report chargeable hours inaccurately for a client engagement. The requirements and application material set out in Section 270 apply in these circumstances.

Identifying Threats

300.6 A1 Threats to compliance with the fundamental principles might be created by a broad range of facts and circumstances. The categories of threats are described in paragraph 120.6 A3. The following are examples of facts and circumstances within each of those categories of threats

that might create threats for a professional accountant when undertaking a professional service:

(a) Self-interest Threats

- A professional accountant having a direct financial interest in a client.
- A professional accountant quoting a low fee to obtain a new engagement and the fee is so low that it might be difficult to perform the professional service in accordance with applicable technical and professional standards for that price.
- A professional accountant having a close business relationship with a client.
- A professional accountant having access to confidential information that might be used for personal gain.
- A professional accountant discovering a significant error when evaluating the results of a previous professional service performed by a member of the accountant's firm.

(b) Self-review Threats

- A professional accountant issuing an assurance report on the effectiveness of the operation of financial systems after implementing the systems.
- A professional accountant having prepared the original data used to generate records that are the subject matter of the assurance engagement.

(c) Advocacy Threats

- A professional accountant promoting the interests of, or shares in, a client.
- A professional accountant acting as an advocate on behalf of a client in litigation or disputes with third parties.
- A professional accountant lobbying in favor of legislation on behalf of a client.

(d) Familiarity Threats

- A professional accountant having a close or immediate family member who is a director or officer of the client.
- A director or officer of the client, or an employee in a position to exert significant influence over the subject matter of the engagement, having recently served as the engagement partner.
- An audit team member having a long association with the audit client.

(e) Intimidation Threats

- A professional accountant being threatened with dismissal from a client engagement or the firm because of a disagreement about a professional matter.
- A professional accountant feeling pressured to agree with the judgment of a client because the client has more expertise on the matter in question.
- A professional accountant being informed that a planned promotion will not occur unless the accountant agrees with an inappropriate accounting treatment.

- A professional accountant having accepted a significant gift from a client and being threatened that acceptance of this gift will be made public.

300.6 A2 The use of technology is a specific circumstance that might create threats to compliance with the fundamental principles. Considerations that are relevant when identifying such threats when a professional accountant relies upon the output from technology include:

- Whether information about how the technology functions is available to the accountant.
- Whether the technology is appropriate for the purpose for which it is to be used.
- Whether the accountant has the professional competence to understand, use and explain the output from the technology.
- Whether the technology incorporates expertise or judgments of the firm.
- Whether the technology was designed or developed by the firm and therefore might create a self-interest or self-review threat.

...

SECTION 320 PROFESSIONAL APPOINTMENTS

...

Requirements and Application Material

...

Using the Work of an Expert or the Output of Technology

R320.10 When a professional accountant intends to use the work of an expert or the output of technology in the course of undertaking a professional activity, the accountant shall determine whether the use is appropriate for the intended purpose.

320.10 A1 Factors to consider when a professional accountant intends to use the work of an expert include the reputation and expertise of the expert, the resources available to the expert, and the professional and ethics standards applicable to the expert. This information might be gained from prior association with the expert or from consulting others.

320.10 A2 Factors to consider when a professional accountant intends to use the output of technology include:

- The nature of the activity to be performed by the technology.
- The expected use of, or extent of reliance on, the output from the technology.
- The professional accountant's ability to understand the output from the technology for the context in which it is to be used.
- Whether the technology is established and effective for the purpose intended.
- Whether the new technology has been appropriately tested and evaluated for the purpose intended.

- The reputation of the developer of the technology if acquired from or developed by an external vendor.
- The firm's oversight of the design, development, implementation, operation, maintenance, monitoring or updating of the technology.
- The appropriateness of the inputs to the technology, including data and any related decisions.

...

INTERNATIONAL INDEPENDENCE STANDARDS

(PARTS 4A AND 4B)

PART 4A – INDEPENDENCE FOR AUDIT AND REVIEW ENGAGEMENTS

SECTION 400

APPLYING THE CONCEPTUAL FRAMEWORK TO INDEPENDENCE FOR AUDIT AND REVIEW ENGAGEMENTS

...

Requirements and Application Material

...

Prohibition on Assuming Management Responsibilities

R400.15 A firm or a network firm shall not assume a management responsibility for an audit client.

400.15 A1 Management responsibilities involve controlling, leading and directing an entity, including making decisions regarding the acquisition, deployment and control of human, financial, technological, physical and intangible resources.

400.15 A2 When a firm or a network firm assumes a management responsibility for an audit client, self-review, self-interest and familiarity threats are created. Assuming a management responsibility might also create an advocacy threat because the firm or network firm becomes too closely aligned with the views and interests of management.

400.15 A3 Determining whether an activity is a management responsibility depends on the circumstances and requires the exercise of professional judgment. Examples of activities that would be considered a management responsibility include:

- Setting policies and strategic direction.
- Hiring or dismissing employees.
- Directing and taking responsibility for the actions of employees in relation to the employees' work for the entity.
- Authorizing transactions.
- Controlling or managing bank accounts or investments.

- Deciding which recommendations of the firm or network firm or other third parties to implement.
- Reporting to those charged with governance on behalf of management.
- Taking responsibility for:
 - The preparation and fair presentation of the financial statements in accordance with the applicable financial reporting framework.
 - Designing, implementing, monitoring or maintaining internal control.

400.15 A4 Subject to compliance with paragraph R400.16, providing advice and recommendations to assist the management of an audit client in discharging its responsibilities is not assuming a management responsibility. The provision of advice and recommendations to an audit client might create a self-review threat and is addressed in Section 600.

R400.16 When performing a professional activity for an audit client, the firm shall be satisfied that client management makes all judgments and decisions that are the proper responsibility of management. This includes ensuring that the client's management:

- (a) Designates an individual who possesses suitable skill, knowledge and experience to be responsible at all times for the client's decisions and to oversee the activities. Such an individual, preferably within senior management, would understand:
 - (i) The objectives, nature and results of the activities; and
 - (ii) The respective client and firm or network firm responsibilities.

However, the individual is not required to possess the expertise to perform or re-perform the activities.

- (b) Provides oversight of the activities and evaluates the adequacy of the results of the activities performed for the client's purpose.
- (c) Accepts responsibility for the actions, if any, to be taken arising from the results of the activities.

400.16 A1 When technology is used in performing a professional activity for an audit client, the requirements in paragraphs R400.15 and R400.16 apply regardless of the nature or extent of such use.

...

SECTION 520

BUSINESS RELATIONSHIPS

...

Requirements and Application Material

General

520.3 A1 This section contains references to the "materiality" of a financial interest and the "significance" of a business relationship. In determining whether such a financial interest is material to an individual, the combined net worth of the individual and the individual's immediate family members may be taken into account.

520.3 A2 Examples of a close business relationship arising from a commercial relationship or common financial interest include:

- Having a financial interest in a joint venture with either the client or a controlling owner, director or officer or other individual who performs senior managerial activities for that client.
- Arrangements to combine one or more services or products of the firm or a network firm with one or more services or products of the client and to market the package with reference to both parties.
- Arrangements under which the firm or a network firm sells, resells, distributes or markets the client's products or services, or the client sells, resells, distributes or markets the firm's or a network firm's products or services.
- Arrangements under which the firm or a network firm develops jointly with the client, products or solutions which one or both parties sell or license to third parties.

...

Buying Goods or Services

520.6 A1 The purchase of goods and services from an audit client by a firm, a network firm, an audit team member, or any of that individual's immediate family does not usually create a threat to independence if the transaction is in the normal course of business and at arm's length. However, such transactions might be of such a nature and magnitude that they create a self-interest threat.

520.6 A2 Examples of actions that might eliminate such a self-interest threat include:

- Eliminating or reducing the magnitude of the transaction.
- Removing the individual from the audit team.

Providing, Selling, Reselling or Licensing Technology

520.7 A1 If a firm or a network firm provides, sells, resells or licenses technology to an audit client, the requirements and application material in Section 600 apply.

...

SECTION 600

PROVISION OF NON-ASSURANCE SERVICES TO AN AUDIT CLIENT

Introduction

600.1 Firms are required to comply with the fundamental principles, be independent, and apply the conceptual framework set out in Section 120 to identify, evaluate and address threats to independence.

600.2 Firms and network firms might provide a range of non-assurance services to their audit clients, consistent with their skills and expertise. Providing non-assurance services to audit clients might create threats to compliance with the fundamental principles and threats to independence.

- 600.3 This section sets out requirements and application material relevant to applying the conceptual framework to identify, evaluate and address threats to independence when providing non-assurance services to audit clients. The subsections that follow set out specific requirements and application material that are relevant when a firm or a network firm provides certain types of non-assurance services to audit clients and indicate the types of threats that might be created as a result.
- 600.4 Some subsections include requirements that expressly prohibit a firm or a network firm from providing certain services to an audit client because the threats created cannot be eliminated and safeguards are not capable of being applied to reduce the threats to an acceptable level.
- 600.5 New business practices, the evolution of financial markets and changes in technology are some developments that make it impossible to draw up an all-inclusive list of non-assurance services that firms and network firms might provide to an audit client. The conceptual framework and the general provisions in this section apply when a firm proposes to a client to provide a non-assurance service for which there are no specific requirements and application material.
- 600.6 The requirements and application material in this section also apply in those circumstances where:
- (a) A firm or a network firm uses technology to provide a non-assurance service to an audit client; or
 - (b) A firm or a network firm provides, sells, resells or licenses technology to an audit client.

...

Requirements and Application Material

General

...

Identifying and Evaluating Threats

All Audit Clients

- 600.9 A1 A description of the categories of threats that might arise when a firm or a network firm provides a non-assurance service to an audit client is set out in paragraph 120.6 A3.
- 600.9 A2 Factors that are relevant in identifying the different threats that might be created by providing a non-assurance service to an audit client, and evaluating the level of such threats include:
- The nature, scope, intended use and purpose of the service.
 - The manner in which the service will be provided, such as the personnel to be involved and their location.
 - The client's dependency on the service, including the frequency with which the service will be provided.
 - The legal and regulatory environment in which the service is provided.
 - Whether the client is a public interest entity.

- The level of expertise of the client's management and employees with respect to the type of service provided.
- The extent to which the client determines significant matters of judgment. (Ref: Para. R400.15 to R400.16).
- Whether the outcome of the service will affect the accounting records or matters reflected in the financial statements on which the firm will express an opinion, and, if so:
 - The extent to which the outcome of the service will have a material effect on the financial statements.
 - The degree of subjectivity involved in determining the appropriate amounts or treatment for those matters reflected in the financial statements.
- The nature and extent of the impact of the service, if any, on the systems that generate information that forms a significant part of the client's:
 - Accounting records or financial statements on which the firm will express an opinion.
 - Internal controls over financial reporting.
- The degree of reliance that will be placed on the outcome of the service as part of the audit.
- The fee relating to the provision of the non-assurance service.

600.9 A3 Subsections 601 to 610 include examples of additional factors that are relevant in identifying threats to independence created by providing certain non-assurance services, and evaluating the level of such threats.

...

Self-review threats

600.13 A1 When a firm or a network firm provides a non-assurance service to an audit client, there might be a risk of the firm auditing its own or the network firm's work, thereby giving rise to a self-review threat. A self-review threat is the threat that a firm or a network firm will not appropriately evaluate the results of a previous judgment made or an activity performed by an individual within the firm or network firm as part of a non-assurance service on which the audit team will rely when forming a judgment as part of an audit.

R600.14 Before providing a non-assurance service to an audit client, a firm or a network firm shall determine whether the provision of that service might create a self-review threat by evaluating whether there is a risk that:

- (a) The results of the service will form part of or affect the accounting records, the internal controls over financial reporting, or the financial statements on which the firm will express an opinion; and
- (b) In the course of the audit of those financial statements on which the firm will express an opinion, the audit team will evaluate or rely on any judgments made or activities performed by the firm or network firm when providing the service.

Audit Clients that are Public Interest Entities

- 600.15 A1 When the audit client is a public interest entity, stakeholders have heightened expectations regarding the firm's independence. These heightened expectations are relevant to the reasonable and informed third party test used to evaluate a self-review threat created by providing a non-assurance service to an audit client that is a public interest entity.
- 600.15 A2 Where the provision of a non-assurance service to an audit client that is a public interest entity creates a self-review threat, that threat cannot be eliminated, and safeguards are not capable of being applied to reduce that threat to an acceptable level.

Self-review threats

- R600.16** A firm or a network firm shall not provide a non-assurance service to an audit client that is a public interest entity if the provision of that service might create a self-review threat in relation to the audit of the financial statements on which the firm will express an opinion. (Ref: Para. 600.13 A1 and R600.14).

...

SUBSECTION 601 – ACCOUNTING AND BOOKKEEPING SERVICES

Introduction

- 601.1 In addition to the specific requirements and application material in this subsection, the requirements and application material in paragraphs 600.1 to 600.27 A1 are relevant to applying the conceptual framework when providing accounting and bookkeeping services to an audit client.

...

Requirements and Application Material

...

Audit Clients that are Not Public Interest Entities

- R601.5** A firm or a network firm shall not provide to an audit client that is not a public interest entity accounting and bookkeeping services, including preparing financial statements on which the firm will express an opinion or financial information which forms the basis of such financial statements, unless:
- (a) The services are of a routine or mechanical nature; and
 - (b) The firm addresses any threats that are not at an acceptable level.
- 601.5 A1 Accounting and bookkeeping services that are routine or mechanical:
- (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 judgment.
- 601.5 A2 Accounting and bookkeeping services can either be manual or automated. In determining whether an automated service is routine or mechanical, factors to be considered include how

the technology functions and whether the technology is based on expertise or judgments of the firm or a network firm.

601.5 A3 Examples of services, whether manual or automated, that might be regarded as routine or mechanical include:

- Preparing payroll calculations or reports based on client-originated data for approval and payment by the client.
- Recording recurring transactions for which amounts are easily determinable from source documents or originating data, such as a utility bill where the client has determined or approved the appropriate account classification.
- Calculating depreciation on fixed assets when the client determines the accounting policy and estimates of useful life and residual values.
- Posting transactions coded by the client to the general ledger.
- Posting client-approved entries to the trial balance.
- Preparing financial statements based on information in the client-approved trial balance and preparing related notes based on client-approved records.

The firm or a network firm may provide such services to audit clients that are not public interest entities provided that the firm or network firm complies with the requirements of paragraph R400.16 to ensure that it does not assume a management responsibility in connection with the service and with the requirement in paragraph R601.5 (b).

601.5 A4 Examples of actions that might be safeguards to address a self-review threat created when providing accounting and bookkeeping services of a routine or mechanical nature to an audit client that is not a public interest entity include:

- Using professionals who are not audit team members to perform the service.
- Having an appropriate reviewer who was not involved in providing the service review the audit work or service performed.

...

SUBSECTION 606 – INFORMATION TECHNOLOGY SYSTEMS SERVICES

Introduction

606.1 In addition to the specific requirements and application material in this subsection, the requirements and application material in paragraphs 600.1 to 600.27 A1 are relevant to applying the conceptual framework when providing an information technology (IT) systems service to an audit client.

Requirements and Application Material

Description of Service

606.2 A1 IT systems services comprise a broad range of services including:

- Designing or developing hardware or software IT systems.

- Implementing IT systems, including installation, configuration, interfacing, or customization.
- Operating, maintaining, monitoring, or updating IT systems.
- Collecting or storing data or managing (directly or indirectly) the hosting of data on behalf of the audit client.

606.2 A2 The IT systems might:

- (a) Aggregate source data;
- (b) Form part of the internal control over financial reporting; or
- (c) Generate information that affects the accounting records or financial statements, including related disclosures.

However, the IT systems might also involve matters that are unrelated to the audit client's accounting records or the internal control over financial reporting or financial statements.

Risk of Assuming Management Responsibility When Providing an IT Systems Service

R606.3 Paragraph R400.15 precludes a firm or a network firm from assuming a management responsibility. When providing IT systems services to an audit client, the firm or network firm shall be satisfied that:

- (a) The client acknowledges its responsibility for establishing and monitoring a system of internal controls;
- (b) The client, through a competent individual, preferably within senior management, makes all management decisions that are the proper responsibility of management with respect to the design, development, implementation, operation, maintenance, monitoring, or updating of the IT systems;
- (c) The client evaluates the adequacy and results of the design, development, implementation, operation, maintenance, monitoring, or updating of the IT system; and
- (d) The client is responsible for operating the IT system and for the data it generates and uses.

606.3 A1 Examples of IT systems services that result in the assumption of a management responsibility include where a firm or a network firm:

- Provides services in relation to the hosting (directly or indirectly) of an audit client's data.
- Operates an audit client's network security, business continuity or disaster recovery function.

606.3 A2 The collection, receipt and retention of data provided by an audit client to enable the provision of a permissible service to that client does not result in an assumption of management responsibility.

Potential Threats Arising from the Provision of IT Systems Services

All Audit Clients

606.4 A1 Providing IT systems services to an audit client might create a self-review threat when there is a risk that the results of the services will affect the audit of the financial statements on which the firm will express an opinion.

606.4 A2 Factors that are relevant in identifying a self-review threat created by providing an IT systems service to an audit client, and evaluating the level of such a threat include:

- The nature of the service.
- The nature of the client's IT systems and the extent to which the IT systems service impacts or interacts with the client's accounting records, internal controls over financial reporting or financial statements.
- The degree of reliance that will be placed on the particular IT systems as part of the audit.

When a self-review threat for an audit client that is a public interest entity has been identified, paragraph R606.6 applies.

606.4 A3 Examples of IT systems services that might create a self-review threat when they form part of or affect an audit client's accounting records or system of internal control over financial reporting include:

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

Audit Clients that are Not Public Interest Entities

606.5 A1 An example of an action that might be a safeguard to address a self-review threat created by the provision of an IT systems service to an audit client that is not a public interest entity is using professionals who are not audit team members to perform the service.

Audit Clients that are Public Interest Entities

R606.6 A firm or a network firm shall not provide IT systems services to an audit client that is a public interest entity if the provision of such services might create a self-review threat (Ref: Para. R600.14 and R600.16).

...

PART 4B – INDEPENDENCE FOR ASSURANCE ENGAGEMENTS OTHER THAN AUDIT AND -REVIEW ENGAGEMENTS

SECTION 900

APPLYING THE CONCEPTUAL FRAMEWORK TO INDEPENDENCE FOR ASSURANCE ENGAGEMENTS OTHER THAN AUDIT AND REVIEW ENGAGEMENTS

Introduction

General

900.1 This Part applies to assurance engagements other than audit engagements and review engagements. Examples of such engagements include:

- Assurance on an entity's key performance indicators.
- Assurance on an entity's compliance with law or regulation.
- Assurance on performance criteria, such as value for money, achieved by a public sector body.
- Assurance on the effectiveness of an entity's system of internal control.
- Assurance on an entity's non-financial information, for example, environmental, social and governance disclosures, including greenhouse gas statements.
- An audit of specific elements, accounts or items of a financial statement.

...

Requirements and Application Material

...

Prohibition on Assuming Management Responsibilities

R900.13 A firm shall not assume a management responsibility related to the underlying subject matter and, in an attestation engagement, the subject matter information of an assurance engagement provided by the firm. If the firm assumes a management responsibility as part of any other service provided to the assurance client, the firm shall ensure that the responsibility is not related to the underlying subject matter and, in an attestation engagement, the subject matter information of the assurance engagement provided by the firm.

900.13 A1 Management responsibilities involve controlling, leading and directing an entity, including making decisions regarding the acquisition, deployment and control of human, financial, technological, physical and intangible resources.

900.13 A2 When a firm assumes a management responsibility related to the underlying subject matter and, in an attestation engagement, the subject matter information of an assurance engagement, self-review, self-interest and familiarity threats are created. Assuming a

management responsibility might create an advocacy threat because the firm becomes too closely aligned with the views and interests of management.

900.13 A3 Determining whether an activity is a management responsibility depends on the circumstances and requires the exercise of professional judgment. Examples of activities that would be considered a management responsibility include:

- Setting policies and strategic direction.
- Hiring or dismissing employees.
- Directing and taking responsibility for the actions of employees in relation to the employees' work for the entity.
- Authorizing transactions.
- Controlling or managing bank accounts or investments.
- Deciding which recommendations of the firm or other third parties to implement.
- Reporting to those charged with governance on behalf of management.
- Taking responsibility for designing, implementing, monitoring and maintaining internal control.

900.13 A4 Examples of assuming a management responsibility in relation to the underlying subject matter and, in an attestation engagement, the subject matter information of an assurance engagement, include:

- Providing services in relation to the hosting (directly or indirectly) of the underlying subject matter or subject matter information.
- Operating an assurance client's network security, business continuity or disaster recovery function related to the underlying subject matter or subject matter information.

900.13 A5 The collection, receipt and retention of data to enable the performance of assurance and non-assurance engagements does not result in an assumption of management responsibility.

900.13 A6 Subject to compliance with paragraph R900.14, providing advice and recommendations to assist the management of an assurance client in discharging its responsibilities is not assuming a management responsibility.

R900.14 When performing a professional activity for an assurance client that is related to the underlying subject matter and, in an attestation engagement, the subject matter information of the assurance engagement, the firm shall be satisfied that client management makes all related judgments and decisions that are the proper responsibility of management. This includes ensuring that the client's management:

- (a) Designates an individual who possesses suitable skill, knowledge and experience to be responsible at all times for the client's decisions and to oversee the activities. Such an individual, preferably within senior management, would understand:
 - (i) The objectives, nature and results of the activities; and
 - (ii) The respective client and firm responsibilities.

However, the individual is not required to possess the expertise to perform or re-perform the activities.

- (b) Provides oversight of the activities and evaluates the adequacy of the results of the activity performed for the client's purpose; and
- (c) Accepts responsibility for the actions, if any, to be taken arising from the results of the activities.

900.14 A1 When technology is used in performing a professional activity for an assurance client, the requirements in paragraphs R900.13 and R900.14 apply regardless of the nature or extent of such use.

...

SECTION 920 BUSINESS RELATIONSHIPS

...

Requirements and Application Material

General

920.3 A1 This section contains references to the "materiality" of a financial interest and the "significance" of a business relationship. In determining whether such a financial interest is material to an individual, the combined net worth of the individual and the individual's immediate family members may be taken into account.

920.3 A2 Examples of a close business relationship arising from a commercial relationship or common financial interest include:

- Having a financial interest in a joint venture with either the assurance client or a controlling owner, director or officer or other individual who performs senior managerial activities for that client.
- Arrangements to combine one or more services or products of the firm with one or more services or products of the client and to market the package with reference to both parties.
- Arrangements under which the firm sells, resells, distributes or markets the client's products or services, or the client sells, resells, distributes or markets the firm's products or services.
- Arrangements under which a firm develops jointly with the assurance client, products or solutions which one or both parties sell or license to third parties.

...

Buying Goods or Services

920.5 A1 The purchase of goods and services from an assurance client by a firm, or an assurance team member, or any of that individual's immediate family does not usually create a threat to independence if the transaction is in the normal course of business and at arm's length.

However, such transactions might be of such a nature and magnitude that they create a self-interest threat.

920.5 A2 Examples of actions that might eliminate such a self-interest threat include:

- Eliminating or reducing the magnitude of the transaction.
- Removing the individual from the assurance team.

Providing, Selling, Reselling or Licensing Technology

920.6 A1 If a firm provides, sells, resells or licenses technology to an assurance client, the requirements and application material in Section 950 apply.

...

SECTION 950

PROVISION OF NON-ASSURANCE SERVICES TO ASSURANCE CLIENTS

...

Introduction

950.1 Firms are required to comply with the fundamental principles, be independent, and apply the conceptual framework set out in Section 120 to identify, evaluate and address threats to independence.

950.2 Firms might provide a range of non-assurance services to their assurance clients, consistent with their skills and expertise. Providing certain non-assurance services to assurance clients might create threats to compliance with the fundamental principles and threats to independence.

950.3 This section sets out requirements and application material relevant to applying the conceptual framework to identify, evaluate and address threats to independence when providing non-assurance services to assurance clients.

950.4 New business practices, the evolution of financial markets and changes in technology are some developments that make it impossible to draw up an all-inclusive list of non-assurance services that firms might provide to an assurance client. The conceptual framework and the general provisions in this section apply when a firm proposes to a client to provide a non-assurance service for which there are no specific requirements and application material.

950.5 The requirements and application material in this section also apply in those circumstances where:

- (a) A firm uses technology to provide a non-assurance service to an assurance client; or
- (b) A firm provides, sells, resells or licenses technology to an assurance client.

Requirements and Application Material

General

...

Identifying and Evaluating Threats

950.7 A1 A description of the categories of threats that might arise when a firm provides a non-assurance service to an assurance client is set out in paragraph 120.6 A3.

950.7 A2 Factors that are relevant in identifying and evaluating the different threats that might be created by providing a non-assurance service to an assurance client include:

- The nature, scope, intended use and purpose of the service.
- The manner in which the service will be provided, such as the personnel to be involved and their location.
- The client's dependency on the service, including the frequency with which the service will be provided.
- The legal and regulatory environment in which the service is provided.
- Whether the client is a public interest entity.
- The level of expertise of the client's management and employees with respect to the type of service provided.
- Whether the outcome of the service will affect the underlying subject matter and, in an attestation engagement, matters reflected in the subject matter information of the assurance engagement, and, if so:
 - The extent to which the outcome of the service will have a material effect on the underlying subject matter and, in an attestation engagement, the subject matter information of the assurance engagement.
 - The extent to which the assurance client determines significant matters of judgment (Ref: Para. R900.13 to R900.14).
- The degree of reliance that will be placed on the outcome of the service as part of the assurance engagement.
- The fee relating to the provision of the non-assurance service.

...

Self-Review Threats

950.10 A1 A self-review threat might be created if, in an attestation engagement, the firm is involved in the preparation of subject matter information which subsequently becomes the subject matter information of an assurance engagement. Examples of non-assurance services that might

create such self-review threats when providing services related to the subject matter information of an assurance engagement include:

- (a) Developing and preparing prospective information and subsequently issuing an assurance report on this information.
- (b) Performing a valuation that is related to or forms part of the subject matter information of an assurance engagement.
- (c) 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.

Assurance clients that are public interest entities

950.11 A1 Expectations about a firm's independence are heightened when an assurance engagement is undertaken by a firm for a public interest entity and the results of that engagement will be:

- (a) Made available publicly, including to shareholders and other stakeholders; or
- (b) Provided to an entity or organization established by law or regulation to oversee the operation of a business sector or activity.

Consideration of these expectations forms part of the reasonable and informed third party test applied when determining whether to provide a non-assurance service to an assurance client.

950.11 A2 If a self-review threat exists in relation to an engagement undertaken in the circumstances described in paragraph 950.11 A1 (b), the firm is encouraged to disclose the existence of that self-review threat and the steps taken to address it to the party engaging the firm or those charged with governance of the assurance client and to the entity or organization established by law or regulation to oversee the operation of a business sector or activity to which the results of the engagement will be provided.

...

GLOSSARY, INCLUDING LISTS OF ABBREVIATIONS

...

Conceptual framework This term is described in Section 120.

Confidential information Any information, data or other material in whatever form or medium (including written, electronic, visual or oral) that is not in the public domain.

Contingent fee A fee calculated on a predetermined basis relating to the outcome of a transaction or the result of the services performed by the firm. A fee that is established by a court or other public authority is not a contingent fee.

...

The *International Code of Ethics for Professional Accountants (including International Independence Standards)*, Exposure Drafts, Consultation Papers, and other IESBA publications are published by, and copyright of, IFAC.

The IESBA and IFAC do not accept responsibility for loss caused to any person who acts or refrains from acting in reliance on the material in this publication, whether such loss is caused by negligence or otherwise.

The 'International Ethics Standards Board for Accountants, *International Code of Ethics for Professional Accountants (including International Independence Standards)*', 'International Federation of Accountants', 'IESBA', 'IFAC', the IESBA logo, and IFAC logo are trademarks of IFAC, or registered trademarks and service marks of IFAC in the US and other countries.

Copyright © February 2022 by the International Federation of Accountants (IFAC). All rights reserved. Permission is granted to make copies of this work to achieve maximum exposure and feedback provided that each copy bears the following credit line: "*Copyright © February 2022 by the International Federation of Accountants (IFAC). All rights reserved. Used with permission of IFAC. Permission is granted to make copies of this work to achieve maximum exposure and feedback.*"

Published by:





**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