Potential Ethics Impact on the Behavior of Professional Accountants: Independence

Introduction

This publication forms part of the IESBA's Technology Working Group's Phase 2 Report, which documents the impacts of disruptive and transformative technologies on the work of professional accountants, and provides extensive analysis and insights into the ethics dimension of those developments.

Specifically, this publication explores the implications of innovative technologies such as artificial intelligence, blockchain, and cloud computing, as well as related issues such as data governance including cybersecurity, through an ethics lens with a focus on matters in relation to Independence, and provides insights into those issues and the questions they raise..

The Working Group comprises Brian Friedrich, IESBA Member and Chair of the Working Group; Vania Borgerth, IESBA Member; David Clark, IESBA Technical Advisor; Christelle Martin, IESBA Member; and Sundeep Takwani, former IESBA Technical Advisor.

The full Phase 2 Report also discusses the relevance and importance of the overarching principles and specific provisions in the *International Code of Ethics for Professional Accountants (including International Independence Standards)* (the Code) in laying out the ethics guardrails for professional accountants as they face opportunities and challenges in their work as a result of rapid digitalization.

This publication does not amend or override the Code, the text of which alone is authoritative and reading it is not a substitute for reading the Code and is not intended to be exhaustive and reference to the Code itself should always be made. This publication does not constitute an authoritative or official pronouncement of the IESBA.

Potential Ethics Impact on the Behavior of PAs

The following sections of the report focus on the potential ethics impacts of technology on the behavior of PAs: competence and due care, objectivity, transparency and confidentiality, and independence. The Working Group acknowledges that many of the impacts raised by stakeholders during Phase 2 of fact-finding both reaffirm and underscore the outcomes from Phase 1, thereby supporting the IESBA's Technology ED. Other foreseeable impacts or concerns raised by stakeholders are new or extend the Phase 1 findings. These further impacts or concerns form the basis of the Working Group's insights and recommendations, detailed in *Section III: Insights and Recommendations*, with respect to areas of potential enhancement to the Code and topics for non-authoritative guidance for the IESBA's consideration.[1]

Independence

1. When an individual PA, firm, or a network firm provides a non-assurance service (NAS) to an audit client,[2] they need to comply with the International Independence Standards contained in the Code.[3] This requires knowledge, understanding, and the application of all the relevant provisions that apply to all PAs in Part 1, the additional provisions for PAPPs in Part 3, and the specific independence provisions in Part 4A relating to audit and review engagements. This means that they must comply with the general principles-based requirements contained in the Code. Among other matters, these prohibit[4] providing:

(a) NAS that involves assuming a management responsibility.

(b) NAS that creates a threat to independence that is not at an acceptable level and cannot be addressed by:

- Eliminating the circumstance creating the threat (e.g., the proposed service cannot be restructured or its scope otherwise revised); or
- Applying safeguards (e.g., using professionals who are not audit team members to perform the NAS), where available and capable of being applied, to reduce the threats to independence to an acceptable level.

2. Separately, when a firm or a network firm provides an assurance engagement other than an audit or review engagement, Part 4B of the Code applies in addition to Parts 1 and 3. For all assurance engagements, Part 2 of the Code also applies to PAPPs in certain circumstances such as when facing pressure to breach the fundamental principles.

3. For this section of the report, the use of the term "firm" is intended in a broad general context (i.e., with consideration of both a firm and/or a network firm), as opposed to the specific definitions and scope as specified in the Code.

4. Specific to technology-related assurance engagements, stakeholders highlighted three areas of focus in the context of developing, implementing, and using emerging technology:

(a) Management Responsibility: Risks of auditors assuming management responsibility are elevated when they are involved with technology-related assurance engagements (or engagements in heavily technology-dependent organizations).

(b) Self-review Threat: Involvement in certain technology-related NAS activities can lead to new instances of self-review threat – in addition to other threats, such as advocacy and self-interest – compared with other NAS.

(c) Business Relationships: New business lines and relationships are being made possible because of transformational technologies. These have the potential to create self-interest and advocacy threats.

Management Responsibility

5. The Code prohibits a firm or network firm from assuming management responsibility for an audit client. 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. In this regard, stakeholders highlighted four key risk areas in the context of technology use: (1) business insights obtained from data analytics performed during the audit, (2) assuming custody over client data, (3) relying on a firm to support or document organizational processes, and (4) providing cybersecurity assessment services. Each of these areas is discussed below.

(i) Business Insights from Data Analytics

6. Valuable business insights and analytics about an audit client can be uncovered as a side effect of employing sophisticated data analytics during the audit. For example, predictive analysis of the likelihood of default by a debtor provides important audit evidence. Such analysis is also of significant interest to the audit client's credit control staff as they seek to recover debt and make judgments about how credit terms might need to be adjusted.

7. Communicating these business insights to the audit client (e.g., through a management letter or a report to the audit committee) might blur the line between what is typically included in such communications and what is more representative of a business advisory service. This is because predictive data analytics analyze historical data and forecast what is expected to happen based on patterns and behaviors, meaning that the insights obtained in year 1 will be different from the insights obtained a few years later due to the accumulation of patterns and behaviors in data over time.

8. Stakeholders nevertheless observed that such insights are increasingly being requested by client management as deeper insights enable them to ask more relevant questions and make better decisions. This is despite the fact that the audit firm could charge additional non-audit fees (i.e., through providing a NAS by charging for the outputs or selling or licensing the tools themselves) or build strategic rapport with management. In particular:

(a) A regulator noted the increased risk of a firm inadvertently providing more detailed insight than is appropriate over a number of years (i.e., the potential for "scope creep"), meaning that the firm might be unaware that it has assumed management responsibility.[5]

Other stakeholders observed that clients sometimes use audit information for purposes different than the auditor intended, which once again can lead to an assumption of management responsibility that the firm might not be aware of, and thus not under the firm's control.

(b) Another regulator highlighted an emerging risk if firms offer these data analytical tools to the entities they audit, or to entities that might become audit clients in the future.[6] A conflict might arise if the entity uses these tools to analyze data that later becomes subject to the firm's audit.[7]

9. Stakeholders also noted that although the use of data analytics enables firms to dive deeper into data and other information, it appears to detract from proper documentation of conclusions drawn from the data analytics insights as is required when performing an audit.

(ii) Custody of Data

10. As services are increasingly performed "online" by firms, this will often lead to a firm storing, or having custody of, client data. In this regard, stakeholders stressed that there is a responsibility for PAs, and more specifically auditors, to be responsible for safeguarding the data while in the firm's custody. Stakeholders also stressed firms' responsibility to return the data to the client and/or appropriately deleting it from their storage once the service is completed. Stakeholders drew parallels between the custody of client data and the existing Code requirements around custody of client assets,[8] noting that the same basic principles regarding stewardship and restrictions over the custody should apply. The Working Group notes that this issue goes beyond the independence consideration of assuming management responsibility in audit and other assurance engagements. Rather, this issue will also have ethics considerations that impact both PAPPs and PAIBs, given that data is the foundation of all financial and non-financial (e.g., sustainability) reporting. See also Recommendation C of *Section III: Insights and Recommendations*.

(iii) Reliance on a Firm

11. Stakeholders also contemplated a situation where a firm performs assurance work for a client that has limited processes in place around implementing a technology tool or system, and the firm provides assistance to identify and document the client's controls. The extent of client versus firm involvement in this activity would clearly be a factor in determining whether it would be considered a management responsibility. But stakeholders questioned the point at which this occurs, particularly as observed control weaknesses would be communicated to the client as part of the auditor's management letter.

12. A potential concern was also raised where a client uses third-party technology tools with the firm's assistance and the firm understands the tools better than the client, resulting in the client becoming over-reliant on the firm and/or the tool.

(iv) Cybersecurity Assessment Services

13. When a firm provides a cybersecurity assessment service to a client, it cannot assume management responsibility. It was noted that the frequency of such services is a factor in determining whether a management responsibility has been assumed (i.e., the more frequent the cybersecurity service, the more likely the firm might be considered to be assuming management responsibility). To mitigate this risk, the service contract would likely need to include a "walk-away" clause.[9] Such a clause presents a significant concern to clients in relation to a trusted service, such as cybersecurity monitoring, especially when the ongoing service is embedded into a client's ecosystem. The clause is triggered when the client becomes an audit client, and there is an immediate need for the firm to walk away, making audit firms less attractive to clients in providing such services.

14. Some stakeholders advocated for firms to be permitted to do more to help clients, including audit clients. The argument was advanced that some firms bring considerable expertise in specialist services. These include, for example, cybersecurity audits or establishing blockchain e-commerce platforms. The stakeholders argued that the benefits for audit clients (and the public interest) from permitting an audit firm to perform such engagements for audit clients might exceed the risk to auditor independence. Note that this is not a view presently supported by the Code.

Self-review Threat

15. When a firm or a network firm provides a NAS 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.[10] The Code's NAS provisions highlight that it is impossible to draw up a comprehensive list of NAS that firms might provide to an audit client due to the emergence of new business practices, the evolution of financial markets, and changes in technology. However, the conceptual framework and the general NAS provisions apply.

16. Stakeholder outreach suggested that a self-review threat might be created where a firm provides NAS[11] either through employing a technology tool or, more critically, selling or licensing a technology tool that performs the NAS.[12] The Working Group notes the results from the IESBA's 2020 Impact of Technology on Auditor Independence survey which indicate that 24% of respondents did not believe that existing NAS provisions are relevant when a firm sells or licenses technology that performs a NAS, as opposed to firm personnel performing the same NAS. To address this misconception, the revisions arising from the Technology Project explicitly clarify this matter.

17. Nevertheless, appropriately identifying self-review threats when a NAS is being performed by either a technology product or firm personnel is critical because this will have varying impacts on the "permissibility" of the NAS. For example, numerous firms sell or license technology that performs a NAS, such as tax preparation services, that are "permissible" under the NAS provisions. However, when selling or licensing technology that performs other NAS (such as data analytics to support internal audit, a valuation modelling tool to support acquisitions, or an AI screening tool to support recruiting activities), identifying self-review threats, in addition to evaluating the potential for assuming a management responsibility, will be highly dependent on the facts and circumstances. This will require the appropriate exercise of professional judgment.[13]

18. Firms are prohibited from providing many NAS to audit clients, in particular clients that are public interest entities (PIEs), under the revised NAS provisions. This prohibition arises generally from either assuming a management responsibility or the risk of a self-review threat, or both. Nevertheless, stakeholders highlighted some scenarios that they increasingly encounter when considering independence and/or conflict of interest issues from emerging technologies, but where they acknowledge that the Code generally provides sufficient clarity:

(a) For smaller firms, it is challenging to have completely distinct teams that perform the audit engagement versus a NAS for a particular audit client as a safeguard[14] to address the risk of a self-review threat, as such firms have fewer staff resources.

However, it was stressed that regardless of the size of a firm, where NAS is delivered – using or augmented by technology or otherwise – firms should implement appropriate measures to ensure independence. For example, this might include putting in place policies, procedures, and training programs to help promote consistent application of the revised NAS provisions and related safeguards in the Code.

(b) When a firm provides an internally developed technology-related NAS product to a non-audit client that subsequently becomes an audit client, or where such product is later resold or licensed by that non-audit client to one of the firm's audit clients.[15]

Stakeholders shared an example whereby a group of independent firms in a particular jurisdiction is considering jointly developing a data analytics tool to be used for journal entry testing and other analytics. This tool could then be sold to non-audit clients for their internal audit use. It was noted that in this scenario, potential conflict of interest and auditor independence issues should be considered, such as where:

- The client subsequently resells (assuming resale is permissible under the terms of the original sale) or licenses the tool to one of the firms' audit clients.
- The client requests one or more of the firms to operate and manage the tool, and the client later seeks to become an audit client of that firm.

(c) Where firms sell or license automated tools to assist their audit clients with preparing their financial statements, and such tools are also used by the firms in performing the audit; or where the auditor provides or recommends a particular technology system or tool, whether internally developed or not, to the client.

It was acknowledged that the revised NAS provisions address NAS related to accounting and bookkeeping for an audit client.[16] Furthermore, in relation to advice and recommendations, it was noted that IESBA's Q&A publication on the revised NAS provisions will be helpful for firms.

(d) An increasing demand for assurance around whether an entity's technology system (either for financial and/or non-financial reporting) is operating as intended. Whether such an entity is an audit client or will become an audit client in the future are important independence considerations in this regard.

(e) The importance of understanding and knowing who the end users are, or will be, when a technology-related NAS is provided (e.g., through reselling or licensing arrangements), and whether an end user is an audit client will impact independence.

19. Finally, stakeholders noted that both NAS and assurance engagements for environmental, social, and governance (ESG) systems implementation and reporting are increasingly requested by entities. Such sustainability-related engagements might be performed by the entity's existing audit firm. For example, stakeholders observed that clients might engage their audit firms to have their sustainability systems implemented. In this regard, it was questioned whether engaging the same firm to conduct assurance on the outputs from such systems creates an independence issue.[17] The importance of appropriate safeguards[18] and transparency[19] around such scenarios was stressed. As non-financial reporting becomes commonplace, stakeholders also observe that considerations have arisen over where the "line" between non-financial and financial information and internal controls sits.

Business Relationships

20. Broadly speaking, a business relationship can consist of any commercial arrangement between entities. In this regard, business relationships in the form of strategic partnerships between accounting firms and large technology companies are increasingly observed. Such "new economy" business relationships are expected to continue to grow. Accordingly, stakeholders question how the role of the auditor and auditor independence issues will evolve and are interested in whether existing Code provisions[20] are sufficient in this developing context. For example, many terms used in commercial relationships do not translate directly to accounting industry terminology, making it challenging for PAs to navigate already complicated agreements and situations.

21. Stakeholders also raised other examples of technology-related business relationships that might, depending on the specific facts and circumstances, create independence-related issues. These include:

(a) When a firm is engaged to develop an app for a client that initially does not generate revenue for the client, perhaps because it is for internal use, but later the client decides to license the app externally to generate revenue.

(b) When a discount to purchase a particular technology tool or application (such as a commercial accounting package) is shared with a client, or the tool or application is specifically recommended to a client.

Endnotes

1 In considering the Working Group's recommendations detailed in Section III of this report, the IESBA will, when prioritizing future projects and initiatives, also take into account and balance other considerations such as responses from the 2022 Strategy Survey, findings from its recently completed benchmarking initiative, its pre-commitments, and resources available.

2 In Part 4A of the Code, the term "audit" applies equally to "review."

3 The revised NAS provisions will become effective for audits of financial statements for periods beginning on or after December 15, 2022. They replace Section 600, *Provision of Non-Assurance Services to an Audit Client* and include, among others, consequential revisions to:

- Section 400, *Applying the Conceptual Framework to Independence for Audit and Review Engagements*
- Section 525, *Temporary Personnel Assignments*

In this regard, a Questions and Answers (Q&A) publication has been issued by the Staff of the IESBA which is intended to assist NSS, PAOs, and PAPPs (including firms) as they adopt and implement the revisions to the NAS provisions of the Code.

4 A high-level overview of the prohibitions in the Code, *Summary of Prohibitions Applicable to Audits of Public Interest Entities* is available on the IESBA website.

5 UK FRC report on using technology to enhance audit quality: "Technological Resources Using Technology To Enhance Audit Quality." *FRC*, December 2020, https://www.frc.org.uk/getattachment/352c4cc5-60a3-40d0-9f70-a402c5d32ab2/Technological-Resources-Using-Technology-To-Enhance-Audit-Quality_December-2020.pdf (page 14).

6 NZ FMA report on use of new technology and risk to auditor independence: "Audit Quality Monitoring Report 2020." *FMA*, 2020, https://www.fma.govt.nz/assets/Reports/Audit-Quality-Monitoring-Report-2020.pdf (page 14).

7 "Ethical Leadership in a Digital Era: Applying the IESBA Code to Selected Technology-related Scenarios." *Japanese Institute of CPAs and IFAC*, September 2022, https://www.ethicsboard.org/publications/ethical-leadership-digital-era-applying-iesba-code-selected-technology-related-scenarios.

8 Section 350 of the Code

9 A walk-away term in a contract could include, for example, the ability to turn over the responsibility to provide the service to a different firm of equivalent quality, integration, client knowledge, and potentially even comparable pricing for the remainder of the contract.

10 A self-review threat is the threat that a firm will not appropriately evaluate the results of a previous judgment made or an activity performed by an individual within the firm as part of a NAS on which the audit team will rely when forming a judgment as part of an audit.

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

(a) The results of the NAS 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 NAS.

12 See, for example, Cohn, Michael. "PwC rolls out tax and accounting AI apps." *Accounting Today*, 24 February 2021, https://www.accountingtoday.com/news/pwc-rolls-out-tax-and-accounting-ai-digital-apps.

13 *Supra* note 164

14 The revised NAS provisions considered the appropriateness of NAS safeguards [again], following the Safeguards project and related enhancements to the Code. See NAS Basis for Conclusions (para. 78 to 84). In the case of audit clients that are not PIEs (e.g., many SMEs which SMPs will audit), the IESBA determined that the examples of NAS safeguards should be retained because they are capable of addressing threats to independence. In addition, withdrawing them would have significant adverse consequences for audits of non-PIEs (e.g., increased costs and additional complexities that might arise if the audit firm is required to engage another firm to review the outcome or result of the NAS). In evaluating the effect on the public interest, it is relevant to take account of the economic significance of enabling growth of SMEs, rather than increasing their regulatory burdens.

15 Paragraphs R400.30 to R400.32 of the revised NAS provisions

16 Subsection 601 of the revised NAS provisions.

17 See revisions arising from the Technology Project to Part 4B which highlights that this scenario creates a self-review threat. Additionally, in June 2022, the IESBA unanimously resolved to take timely action to develop ethics and independence standards to support transparent, relevant and trustworthy sustainability reporting – "IESBA Commits to Readying Global Ethics and Independence Standards Timely in Support of Sustainability Reporting and Assurance." *IESBA*, 13 June 2022, https://www.ethicsboard.org/news-events/2022-06/iesba-commits-readying-global-ethics-and-independence-standards-timely-support-sustainability.

18 That is, are different teams within the same firm doing the financial statement audit, sustainability systems implementation, and sustainability assurance work on the system, sufficient?

[19] In such circumstances, under the revised NAS provisions (paragraph 950.11 A2), if the client is a PIE and the results of such service will be provided to an oversight body established by law or regulation, then the firm is encouraged to disclose (a) the existence of that self-review threat, and (b) the steps taken to address it. The disclosure is to the party engaging the firm or TCWG 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.

[20] The Code defines a "close business relationships" and prohibits material close business relationships. The revisions arising from the Technology Project also included additional examples of technology-related close business relationships.

ABOUT THE IESBA

The International Ethics Standards Board for Accountants (IESBA) is an independent global standard-setting board. The IESBA serves 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 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).

KEY CONTACTS

Brian Friedrich, IESBA Member and Chair of the Technology Working Group (brian@friedrich.ca)

Ken Siong, Program and Senior Director, IESBA (kensiong@ethicsboard.org)

Kam Leung, Principal, IESBA (kamleung@ethicsboard.org)

IESBA International Ethics Standards Board for Accountants®

www.ethicsboard.org @ethics_board company/iesba

Published by International Federation of Accountants (IFAC), 529 Fifth Avenue, New York, NY 10017