Agenda Item 4-A

DRAFT

IESBA TECHNOLOGY WORKING GROUP
FINAL PHASE 2 REPORT

September 2022

The IESBA Technology Working Group:

Brian Friedrich, IESBA Member (Chair)

Vania Borgerth, IEBSA Member

David Clark, IESBA Technical Advisor

Christelle Martin, IESBA Member

Sundeep Takwani, former IESBA Technical Advisor

The Working Group would like to acknowledge the contributions made throughout Phase 2 by Johanna Field, IAASB Technical Advisor and liaison to the Working Group and Laura Friedrich, IESBA Technical Advisor. Excellent guidance and review commentary on Part II of this report was provided by members of the IESBA Technology Experts Group. Additionally, the Working Group wishes to recognize the invaluable IESBA staff support provided by Kam Leung, Principal, Diane Jules, Director, and Ken Siong, Program and Senior Director.

Contents

EXECUTIVE SUMMARY 3

I. BACKGROUND 7

II. KEY THEMES OBSERVED 11

A. Public Interest Accountability of PAs 11

B. Technology Landscape 17

C. Potential Ethics Impact on the Behavior of PAs 44

D. Multidisciplinary Teams 64

E. Standards and Guidance 66

III. INSIGHTS AND RECOMMENDATIONS 66

IV. SUGGESTIONS FOR THE FUTURE OF THE IESBA'S TECHNOLOGY INITIATIVE 78

APPENDIX I: SUMMARY OF OUTREACH, EVENTS, PRESENTATIONS AND PANEL DISCUSSIONS 80

APPENDIX II: SUGGESTED NON-AUTHORITATIVE RESOURCES AND MATERIALS 88

EXECUTIVE SUMMARY

1. In accordance with the Phase 2 Terms of Reference of the IESBA's technology initiative, the Technology Working Group (Working Group) conducted fact finding in a number of focus areas to identify and assess the potential impact of technology on the behavior of professional accountants (PAs) on the relevance and applicability of the IESBA's *International Code of Ethics for Professional Accountants (including International Independence Standards)* (the Code). The focus areas included robotic process automation (RPA), artificial intelligence (AI), blockchain, cloud computing, and data governance, including cybersecurity.

2. In addition to desk research, the Working Group considered a balanced and diverse set of perspectives, professional and business roles, and experiences from a variety of stakeholders through its targeted outreach.[1] The key PA ethics-related points arising from such outreach were distilled and synthesized into the eight key themes, as outlined in *Section II: Key Themes Observed* of this report. These key points were also analyzed and evaluated against the Code to determine whether they have the potential to impact the Code or the IESBA's work more broadly.

CONCLUSION

3. The Working Group notes that the key themes observed during both Phase 1 (2019-2020) and this second Phase (2021-2022) of its fact-finding have become increasingly consistent over time. The broad insights gathered also remain relevant despite the different types of technology being assessed and evaluated.

4. Specifically, the technology landscape, although dynamic and evolving, has not seen a revolutionary turn that would significantly impact the relevance of the Code. Rather, the findings of Phase 2 underpin the fact that, with few exceptions, the Code continues to remain applicable and relevant to guide ethical decision-making around a PA's involvement with the design, implementation, or use of disruptive and transformative technologies and related issues.

5. The expected finalization of the proposed technology-related revisions to the Code in early 2023 will additionally enhance the Code's robustness and expand its relevance in this environment. Also, the IESBA's careful consideration of the Working Group's Phase 2 recommendations, as outlined in *Section III: Insights and Recommendations* of this report, will help ensure the Code's continued relevance as technology reshapes the roles PAs undertake.

SUMMARY OF RECOMMENDATIONS

Data Used for AI training

A. Revise the Code, for example in Subsection 114 *Confidentiality*, to clarify whether firms and organizations may use client or customer data for internal purposes, such as training AI models, and if so the parameters of such use (prior, informed consent; anonymization). Non-authoritative guidance should also be developed to specifically emphasize the expectations for complying with

[1] Including with individuals representing those charged with governance, investors, regulators, public sector and oversight bodies, technologists (software vendors and developers) and professional accountants in business (PAIBs), professional accountancy organizations (PAOs) including national standard setters (NSS), and accounting firms and individual professional accountants in public practice (PAPPs).

the fundamental principle of integrity when using client or customer data for AI training, i.e., obtaining consent that is meaningful, informed, and transparent.

Transparency and Explainable AI

B. Develop further guidance around the importance of transparency and explainability, whether through non-authoritative guidance or in the Code, specific to when a PA relies on or uses transformative technologies (e.g., AI). Such guidance would highlight that PAs cannot abdicate their public interest responsibility and accountability when relying on or using technology (even in highly automated environments).

This additional guidance might explicitly set out expectations for a PA when relying on a technological solution. For example, before relying on a machine learning tool, the PA would be expected to ensure that the tool is explainable (i.e., that they can reasonably understand the rationale for decisions made by the technology). The Working Group believes that the PA need not be the expert who can explain the tool, but should have access to such an expert and should obtain a reasonable understanding to be comfortable with the tool's inputs, processing, and outputs.

Furthermore, consideration should be given to the ethics expectations for PAs when they are involved with developing transformative technology solutions, for example that they be expected to promote the development of explainable systems, particularly in high-stakes applications.

Data Governance, including Custody of Client Data

C. Revise the Code to address the implications of a PA's custody or holding of client data. Such a workstream could be scoped to also include considering threats to compliance with the fundamental principles given the complexity created for PAs who need to remain current with an evolving patchwork of cross- and intra-jurisdictional data privacy laws and regulations, as well as the ethics challenges related to data governance and management (including cybersecurity).

Continue raising awareness of a PA's strategic role in data governance and management (including cybersecurity), and develop educational resources to highlight such role.

Ethical Leadership and Decision-making

D. With a view to the broader expectations for PAs to exhibit and champion ethical leadership and decision-making, develop non-authoritative guidance to emphasize the potential actions a PA might take when applying the conceptual framework and complying with the Code's fundamental principles in technology-related scenarios relevant across various PA roles and activities.

Communication with Those Charged With Governance (TCWG)

E. To strengthen the concepts of transparency and accountability, add new material to the Code as part of the subsections on "communication with TCWG" in Parts 2 and 3 to encourage, or require, meaningful communication with TCWG by PAs (including individual PAPPs and firms)

about technology-related risks and exposures that might affect PAs' compliance with the fundamental principles and, where applicable, independence requirements.

Reliance on, or Use of, Experts

F. Develop non-authoritative guidance and/or revise the Code in paragraphs 220.7 A1 and 320.10 A1 to emphasize the importance of a PA assessing the extent to which an expert being used and relied upon behaves in alignment with the Code's fundamental principles, and the factors to consider in making such an assessment.

Threshold for "Sufficient" Competence

G. Engage more actively with other bodies, such as IFAC's International Panel on Accountancy Education (IPAE) and PAOs, to encourage them to arrange educational activities to raise awareness about the characteristics of "sufficient" competence in the context of the Code and the International Education Standards (IESs). Such other bodies are better placed to develop non-authoritative guidance to illustrate and emphasize how the Code's principles apply when determining sufficient competence.

Pressure on PAs

H. Revise the Code, for example within Section 270 *Pressure to Breach the Fundamental Principles*, to include illustrations of pressures on PAs (such as time and resourcing constraints; competence gaps; complexity of technology, laws and regulations; pace of change; uncertainty, etc.). In addition, consider revising the description of the intimidation threat (paragraph 120.6 A3(e)) to encompass this broader manifestation of pressure beyond that exerted by another person.

In addition, advocate to PAOs and other bodies, such as IFAC's IPAE, the development of additional non-authoritative resources to raise awareness of, and provide guidance on, how PAs can manage sustained pressures.

Business Relationships

I. Given the rise in strategic and commercial relationships between accounting firms and technology and other companies, revise Section 520 *Business Relationships* more comprehensively to address potential threats to the fundamental principles and, where relevant, independence, in the context of broader business relationships and new forms of relationships that are emerging.

Broader Implications on IESBA's Work

J. Continue initiatives to advocate the importance and relevance of Code, as well as to develop, facilitate the development of, and/or contribute to non-authoritative resources and materials. Appendix II of this report summarizes the pertinent technology-related topics that would particularly benefit from additional non-authoritative guidance to draw out potential ethics issues that might arise and how the Code applies in such scenarios.

SUGGESTED NEXT STEPS

6. Finally, it is clear that technology is not "one and done" and that innovations of technology should continue to be monitored by the IESBA. As such, the Working Group suggests a four-pillar approach, as outlined in *Section IV: Suggestions for the Future of the IESBA's Technology Initiative* of this report, for the IESBA to consider, with a re-evaluation in December 2023.

I. BACKGROUND

History of the IESBA's Technology Initiative

1. The IESBA's Technology Initiative is a high priority, as outlined in the IESBA's *2019-2023 Strategy and Work Plan*. In December 2018, recognizing the breadth and dynamism of technology and its significant impact on the accountancy profession, the IESBA determined to take a systematic, risk-based, and phased approach[2] to explore the ethics implications of technological developments on the accounting, assurance, and finance functions, and identify actions to respond to stakeholder expectations.

2. Phase 1 of the Initiative commenced in December 2018 and focused on the impacts of AI, big data, and data analytics on the ethical behavior of PAs, culminating in the February 2020 Phase 1 Report. The Phase 1 Report set out for the IESBA's consideration:

   - Seven sets of recommendations for enhancing the *International Code of Ethics for Professional Accountants (including International Independence Standards)* (the Code).
   - Additional recommendations for Phase 2 of the Initiative, including two distinct work streams, each with a different focus and remit, led by:
     (i) A Technology Task Force to consider, through a formal standard-setting project, potential enhancements to the Code based on the Phase 1 recommendations; and
     (ii) A Technology Working Group to focus on:
       - Continued information gathering and analysis of transformative technologies (beyond AI, big data, and data analytics) with potential ethical impacts on PAs and the Code ("Phase 2[3] fact-finding").
       - Developing or facilitating the development of non-authoritative guidance material.
       - Coordination with the International Auditing and Assurance Standards Board's (IAASB) Technology Working Group.

2. Informed by the Phase 1 report, the IESBA in:

   (a) March 2020 established the Technology Task Force, which commenced the project[4] to develop enhancements to the Code. In February 2022, the IESBA issued its Exposure Draft: *Proposed*[5] *Technology-related Revisions to the Code* (Technology ED);

---

2 December 2018 IESBA Meeting Agenda Item 7 paragraph 5 and SWP (2019-2023) Basis for Conclusions paragraph 34

3 The Phase 1 Final Report (page 30) recommended the following technology-related topics be considered as priorities for Phase 2: Blockchain, Cryptocurrencies and Initial Coin/Security Token Offerings; Cyber-crime and Cyber-security; Internet of Things; and Data governance. In addition, the approved Project Proposal for the Technology Task Force (paragraph 7) also includes Cloud-based Services as a topic to be considered under Phase 2.

4 As noted in the IESBA's April 2021 Update and the Technology ED issued in February 2022, the technology-related revisions to the Code were developed in a holistic and principles-based manner to encompass all technologies (including AI and machine learning, blockchain, and other future technologies not yet known), in order to preserve and expand the relevance of the Code as technology evolves.

5 Among other matters, the proposals:

- Draw special attention to the professional competence and confidentiality imperatives of the digital age.

(b) December 2020 approved establishing a new Technology Working Group (Working Group) to focus on both developing non-authoritative guidance material and conducting additional fact finding into technology with potential ethics impacts on PAs; and

(c) In March 2021 approved the Working Group's terms of reference.

Working Group Objectives

3. The objectives of the Working Group are:

(a) To develop, or facilitate the development of, non-authoritative resources or materials on technology-related topics that would benefit PAs and the wider stakeholder community[6] through (i) raising their awareness of the ethical implications of technology-related developments for PAs; and/or (ii) supporting PAs in consistently applying the Code in addressing related ethical dilemmas or conflicts, including with respect to independence; and

(b) To identify and assess the potential impact of technology on the behavior of PAs and the relevance[7] and applicability of the Code.

Phase 2 Fact-finding Activities and Process

4. The Working Group's fact-finding activities that informed the key themes observed in this report mainly involved:

- Developing a Briefing Paper to raise awareness of the Working Group's role and activities, and to provide a basis for, and facilitate, structured and consistent stakeholder outreach.
- Targeted outreach, roundtables and events, and panel discussions with a diverse[8] range of stakeholders on ethics-technology issues. See Appendix I for a summary list.
- Desktop research consisting of a review of existing reports, articles, and other publications and media, as well as attending numerous webinars and conferences on relevant topics.
- Establishing the Technology Experts Group[9] (TEG) to act as a "sounding board" for the Working Group, as well as providing advice and other technology expertise as inputs for

---

- Address the ethical dimension of PAs' reliance on, or use of, the output of technology in carrying out their work.
- Further enhance considerations relating to threats from the use of technology as well as considerations relating to complex circumstances in applying the Code's conceptual framework.
- Strengthen and clarify the International Independence Standards (IIS) with respect to technology-related non-assurance services (NAS) firms may provide to their audit clients or technology-related business relationships they may enter into with their audit clients.
- Explicitly acknowledge that the IIS that apply to assurance engagements are applicable to assurance engagements on non-financial information, for example, environmental, social, and governance (ESG) disclosures.

6 In this regard, see the Working Group's Technology Focus Webpage which compiles resources from across the world (including those that the Working Group contributed to developing) to assist both professional accountants in business (PAIBs) and in public practice (PAPPs), including auditors, navigate the ethical challenges and opportunities arising from evolving technologies.

7 For example, modernization of terms and concepts in addition to those recommended in the Phase 1 Final Report, page 23

8 Including different professional roles and perspectives (such as PAIBs and individual PAPPs, firms, PAOs, NSS, regulators, investors, those charged with governance (TCWG), academics, and technologists (i.e., IT professionals), as well as geographic representation

9 Eight members with practical experience in using and implementing technology.

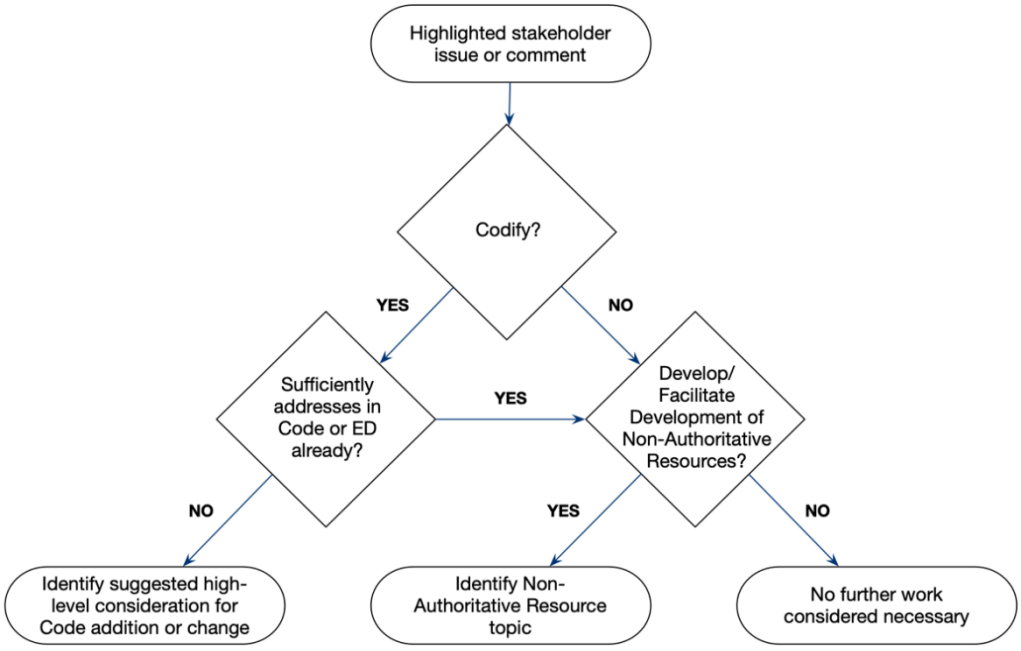
consideration (such as technology-related use cases for the Working Group to consider against the Code).

- Coordinating with, and receiving input from, representatives of the IAASB's Technology Initiative and IFAC's IPAE.
- Interacting with other presenters and panelists both before and during events hosted by other organizations.

5. The meeting notes generated from the targeted outreach related to a particular meeting were sent back to the stakeholders interviewed to ensure fair representation of their comments and obtain their agreement as to the key messages the Working Group took away. To ensure frank dialogue, outreach participants were informed that none of their comments would be specifically attributed to them or their organizations, but rather would be aggregated with the sum of the Working Group's outreach and the evaluation thereof.

6. Once the outreach was substantially complete, the Working Group identified the PA ethics-related points arising from the outreach. These items were then distilled and synthesized into the eight key themes, as outlined in *Section II: Key Themes Observed* of this report. This section also benefitted from review comments by the TEG.

7. Separately, these highlighted items, as well as the use cases provided by the TEG and others, were considered in the context of the Code,[10] analyzed, and evaluated against the following decision process to determine whether they have the potential to impact the Code or the IESBA's work more broadly:



[10] Extant Code as of 2021 (including the revised NAS provisions) along with consideration of the proposals contained in the Technology ED issued on February 18, 2021 with comments due by June 20, 2022. Stakeholder feedback on the ED proposals will be considered by the Task Force and the revisions are anticipated to be finalized, at the latest, by March 2023.

8. The insights arising from the Working Group's analysis and evaluation and resulting recommendations for the IESBA and its various workstreams to consider, are detailed in *Section III: Insights and Recommendations* of this report.

9. Lastly, the Working Group considered the future of the IESBA's Technology Initiative based on the nature and extent, as well as the outcomes, of the substantive fact-finding work completed in both Phases 1 and 2, in addition to the anticipated finalization of the proposed technology-related revisions to the Code in early 2023. In further noting that technology is not a "one and done" endeavor, the Working Group has outlined suggestions for the IESBA to consider in *Section IV: Suggestions for the Future of IESBA's Technology Initiative*.

10. [In finalizing this report, the Working Group has considered the views and feedback from the IESBA and the IESBA Consultative Advisory Group (CAG) in September 2022.] The insights and recommendations contained in the report were also shared with the Technology Task Force, other IESBA workstreams, and the IAASB's technology workstream, as appropriate.

Purpose of the Report and Intended Audience

11. The primary purpose of this report is to provide the IESBA with a comprehensive summary of the Working Group's Phase 2 activities in meeting the Working Group's objectives. To this end, the report presents a summary of the most pressing emerging, disruptive, and transformative technologies – based on both stakeholder interviews and desk research; how stakeholders are experiencing the impact of such technology, and its effect on PA behavior and ethical decision-making; and the Working Group's analysis and evaluation of the potential Code implications and recommended next steps as a result of such findings.

12. In the broader context, this report also provides the IESBA's stakeholders with specific insights as to how innovative technologies are reshaping the professional and business world in which PAs operate. This includes highlighting (a) opportunities for stakeholders globally (such as PAOs, NSS, and regulators) to take a leadership position in those areas stakeholders believe are important, and (b) beneficial topics for non-authoritative resources and materials to help guide this transformation of the profession from an ethics perspective.

Interactions with Other IESBA Workstreams and the IAASB

Technology Task Force and Other IESBA Workstreams

13. The Working Group shared its preliminary observations and insights with the Technology Task Force and these were considered by the Task Force in finalizing its technology-related ED proposals in December 2021. The IESBA-approved technology-related proposals were issued in February 2022. The proposals respond to a public interest need for timely enhancements to the Code in light of the rapid pace of change in, and use of, technology (see paragraphs 58 to 59 of the Technology ED Explanatory Memorandum). In finalizing this report, the Working Group's relevant insights and recommendations were shared with the Task Force for its consideration within the context of its analysis of comment letters received on the Technology ED and assessment of whether further revisions to the Code are appropriate at this time.

14. Similarly, the Working Group will share relevant insights and recommendations with other IESBA workstreams for their consideration as appropriate.

IAASB-IESBA Coordination Matters

15. Input from representatives of the IAASB's technology initiative was considered throughout Phase 2. In addition, audit and assurance stakeholder observations have been shared with IAASB colleagues as appropriate.

II. KEY THEMES OBSERVED

16. Based on the outreach and desk research undertaken by the Working Group, several key themes emerged in relation to the:

    A. Public interest accountability of PAs;

    B. Technology landscape;

    C. Potential ethics impact on the behavior of PAs (competence, objectivity, transparency, and independence); and

    D. The need for multidisciplinary teams, standards, and guidance.

    These are discussed below. They also include stakeholder thoughts on developing consistent and clear standards in areas outside the IESBA Code. The Working Group notes that although these are outside the IESBA's remit, the comments and ideas are relevant for other standard setting, regulatory, and advocacy bodies (both internal and external to the accounting profession) to consider. The IESBA could support, advocate for, or simply pass on those comments and ideas as input to such other bodies for their consideration.

A. Public Interest Accountability of PAs

Why the Profession Needs to Act

17. Digital technologies and related issues – such as AI) data analytics, robotic process automation, blockchain, cloud computing, and data governance (including cyber-security) – continue to have a transformational impact on organizations, governments, economies, and societies. In particular, the lingering COVID-19 pandemic, which in 2020 upended many working practices and lifestyles and made remote and hybrid work mainstream, has accelerated the adoption of digital platforms, tools, and techniques.[11]

18. Despite this uptake of technology implementation and use, a majority of controllers, financial analysts, accountants, and auditors reported not completely trusting the accuracy of their own organizations' financial data, citing causes such as human error and the vast amount of data flooding the system.[12]

19. Concurrently, the centrality of ethics has become undisputed in a world of repeated crises and transformation, both corporate and financial. There is increasing pressure from investors and other stakeholders to embed ethics in corporate culture, and a growing recognition of ethics as an essential condition for sustainable business models. As such, there is a shift from a general expectation of ethics towards a more vocal demand for proactive ethical intent *and actions*. In particular,

[11] Digital technology use during COVID-19 pandemic: A rapid review (November 2020): https://onlinelibrary.wiley.com/doi/epdf/10.1002/hbe2.242

[12] CFO.com Risk Management: Numbers Don't Lie, Until They Do (March 2019): https://www.cfo.com/accounting-tax/auditing/2019/03/numbers-dont-lie-until-they-do/

stakeholders also observed that there are strong ties between ethical behavior, ethical design of technology, and the incentive structure of individuals involved.

20. Against this backdrop, ethical decision-making has become more important than ever to reinforce public trust in this semi-virtual, dynamic environment. PAs – with their responsibility to act in the public interest and to adhere to ethics principles and professional standards – are therefore well positioned to enhance this trust through their work and the organizations and clients they support. It is, however, observed that:

- Ethics continues to be more frequently considered on the backend of technology development, rather than in the front-end, initial design.[13]

  Stakeholders note that PAs are typically not sufficiently involved in the decision-making process of designing technology products and related services, meaning that they are not in a position to support the ethical fitness-for-purpose development and use of such products and services. Also, even when PAs are involved in the design of technological solutions, technologists and PAs often do not speak the same "language," as most PAs in accounting and internal control functions within enterprises reportedly lack both sufficient competence and experience with emerging technology tools.

- Companies are increasingly seeking 'trust' services, such as assurance over AI systems, data integrity and governance, and sustainability information.

  Despite PAPPs being well positioned to generate this trust through their work and the organizations and clients they support, such assurance is currently predominantly provided by other experts – typically engineering or consulting firms.[14] These providers bring specialty technical competence, but largely do not operate under codes of ethics with robust objectivity-related provisions such as in relation to conflicts of interest and independence as set out in the Code. This creates public interest concerns around the objectivity of the 'assurance' being provided and highlights an area where the profession's ethics and independence foundations can make a better contribution.

21. The environment of declining trust and an increased demand for ethical decision-making at all levels of an organization, coupled with the current under-representation of PAs in both internal decision-making and external assurance of systems, provides a strong call to action and significant opportunities for the profession to focus on its ethics and independence foundations to deliver more trusted professional services to employers and clients.

Ethical Leadership

22. Stakeholders observe that audit committees and risk committees are increasingly being asked about their organizations' consideration of either developing or implementing new technology.[15] In addition,

---

[13] See, for example, Beena Ammanath, "Thinking Through the Ethics of New Tech…Before There's a Problem" (November 9, 2021) Harvard Business Review: https://hbr.org/2021/11/thinking-through-the-ethics-of-new-techbefore-theres-a-problem

[14] Thomson Reuters, "Who should provide ESG assurance?" (August 20, 2021): https://tax.thomsonreuters.com/news/who-should-provide-esg-assurance/

[15] Considerations, for example, include how the transformational technology fits into the company's strategy and its capital expenditures; the appropriateness of the company's enterprise risk management system; and cyberattack impacts on technology assets, policies, and regulator expectations, as well as appropriate cybersecurity insurance.

PAs are seen to be ethical leaders who have an opportunity to uphold and promote integrity and objectivity as part of the ethical guardrails around innovation during their organizations' digital transformation. For example, the Working Group believes that PAs can work with data experts, and can help employers and clients understand where to draw the line or what is ethical behavior when facing an ethics "gray zone" (i.e., under circumstances that are not illegal – perhaps because legislation does not yet exist – and are also ethically ambiguous).[16] PAs can do so by relying on the skills, values and behavior they bring to the professional activities they undertake,[17] including adherence to ethical principles and encouraging an ethics-based culture. It is therefore essential for PAs to be at the decision-making table and to help oversee, or at least participate in, the implementation and ongoing operations related to emerging technologies.

23. It is, however, observed that many PAs are generally not substantially involved in the decision-making process for selecting technologies to be developed or implemented within their organizations.[18] This lack of involvement might be enhanced by PAs being more appropriately upskilled in emerging and innovative technologies and gaining sufficient data fluency so that they can understand the critical concerns and ask the right questions. This will also help ensure the ethics impact of technology deployments will be considered earlier in the process, rather than only post-implementation and on an ad-hoc basis.

24. Nevertheless, it is also observed that where PAs are indeed involved in decision-making (for example, generally small and medium-sized organizations and practices), they might lack the relevant understanding of the technology with which they are dealing. This in turn might result in the potential misidentification of the risks and controls pertaining to such technology and a lack of professional competence to determine if the technology (or its outputs) is appropriate or reasonable. It is noted that the potential for miscommunication with software developers and technologists also increases when PAs are not appropriately skilled.

25. In order for ethics and compliance with laws and regulations – for example, in relation to data privacy, cybersecurity, etc. – to be more fully considered in strategic decisions when organizations contemplate developing, implementing, or using technology, appropriately skilled PAs should be encouraged to be involved during conceptualization and design. In this regard, the Code contains provisions in relation to having an inquiring mind, exercising professional judgment, being aware of bias, and maintaining an appropriate level of professional competence (i.e., including relevant technology upskilling) to enable PAs to be ethical leaders in this area and have a seat at the decision-making table. PAs should also be aware of, and transparent about, the level of competence they

---

[16] See, for example:

- Deloitte "Beyond Good Intentions: Navigating the ethical dilemmas facing the technology industry" (October 2021): https://www2.deloitte.com/us/en/insights/industry/technology/ethical-dilemmas-in-technology.html
- Conversations conducted with executives of 13 companies (7 of which were Fortune 500 companies) across 7 different countries, revealed how business leaders in 2020 are influencing the business environment to encourage responsible use of technology and build organizational capacity to act with ethics – World Economic Forum in collaboration with Deloitte and the Markkula Center for Applied Ethics at Santa Clara University, Whitepaper "Ethics by Design: An organizational approach to responsible use of technology" (December 2020): https://www3.weforum.org/docs/WEF_Ethics_by_Design_2020.pdf

[17] Paragraphs 100.2 and 100.3 of the Code

[18] PA involvement in the decision-making process is more significant in smaller entities or in firms, whereas in larger entities, it tends to be the IT department that drives such implementation.

have with different technologies. Accordingly, at the decision-making table, PAs can add value by, for example:

- Identifying design needs and specifications that can help the business function so that fit-for-purpose tools are built in an ethical and socially responsible manner;
- Proactively considering, during the design process, the potential for unintended consequences;
- Questioning assumptions, including bias, in data and in the design of systems and algorithms, and the processes related to creating and/or collecting data;
- Ensuring appropriate conditions, policies and procedures, and/or systems of quality management are in place and operating effectively so that issues, such as threats to compliance with the fundamental principles of the Code,[19] are identified in a timely manner. This includes having proper documentation requirements so that where an issue arises, it is easier to determine whether it is due to a governance issue where controls need to be strengthened or whether it is symptomatic of a broader ethics issue; and
- Being able to determine whether – and to what extent – reliance on technologists is reasonable.

26. Stakeholders also indicated that the digital age has resulted in inherent cybersecurity and data integrity risks within every organization. Stakeholders also expressed the view that a PA's ethics responsibility should extend to controls over:

- Cyberattack[20] prevention and response plans, to safeguard valuable intellectual property and meet confidentiality and privacy requirements; and
- Data governance – along the complete data-to-decision chain, including being able to cull relevant and reliable data and information from what is frequently an 'overload' of available sources.

27. When issues arise, there is an expectation for PAs to take action. In particular, stakeholders stressed the importance of PAs having the moral courage to speak up when there is pressure to breach the fundamental principles in the context of developing, implementing, or using emerging technologies. This includes educating others on ethics issues in technology and fostering a business culture where it is safe to raise issues and concerns. For example, a safe environment should be fostered for others in the organization, such as data scientists, to escalate concerns about any bias or discrimination identified in AI systems without the fear of retaliation.[21]

28. Finally, some stakeholders noted the importance of not conflating professional ethics with morality. For example, considering the merits of PAs working for legitimate enterprises in industries that some people might consider objectionable, such as weapons manufacturers or bioengineering companies, was deemed more a question of individual morals than professional ethics. Nonetheless, due care in

---

19 Section 110 *The Fundamental Principles* of the Code

20 See also, for example, Center for Audit Quality, *The CPA's Role in Addressing Cybersecurity Risk* (May 24, 2017): https://www.thecaq.org/cpas-role-addressing-cybersecurity-risk/. Note also that the Working Group believes this should now include establishing ransomware polices and having back-up IT security teams on standby.

21 See ex-co lead of Google's Ethical AI team who allegedly was fired over a dispute in relation to a research paper she had co-authored. The paper contended that AI systems aimed at mimicking human writing and speech do not exacerbate historical gender biases and use of offensive language (December 2020): https://www.theguardian.com/technology/2020/dec/04/timnit-gebru-google-ai-fired-diversity-ethics

evaluating the implications of decision-making on professional ethics (i.e., identifying, evaluating, and addressing threats to complying with the fundamental principles) is still expected, regardless of the organization.

Shared Responsibility

29. In most instances, technology – even related to management processes and financial reporting systems – is not solely under the PA's control, and consideration is needed to determine how responsibility for such systems should, or can, be shared with other professionals.

30. For example, when technology is developed by a third party to help deliver a service, stakeholders have questioned where the liability resides if technology is implemented and fails to detect certain issues in the organization, makes an inappropriate recommendation, or leads to a breach of confidentiality or privacy, etc. In such circumstances, it was questioned whether liability would reside with the technology designer, the PA who accepted the output of the technology, the CFO, or the auditor who provided assurance on the system or its outputs.[22]

31. Some stakeholders encouraged the concept of shared responsibility, namely that it is the responsibility of everyone involved, including PAs and IT professionals (e.g., data scientists, technologists, and engineers). The degree of responsibility would also be expected to change depending on the position of the individual in the organization, commensurate with their authority and role. Stakeholders view that such shared responsibility is most effectively communicated by the tone at the top, through a robust code of conduct and implicit in a strong ethical organizational culture. In addition, accountability mechanisms for the technology solution's output should be defined upfront, whether this relates to the data forming an input to the system, the algorithms being applied to data, or how the outputs are interpreted and evaluated.

32. Other stakeholders noted that PAs (e.g., the accounting and finance functions of an organization) are ultimately responsible for all aspects of the related accounting and financial reporting system(s), even if such systems are developed and/or maintained by a third-party. For example, where an organization has outsourced its data storage to a third-party provider, and despite there being a joint legal liability for a cyberattack, the audit committee would likely still view the responsibility to be largely on the organization itself (i.e., shared between PAs and the IT department), as opposed to the third-party provider.

33. Nevertheless, it is noted that effectively considering ethics and potential unintended consequences of the technology development or selection process, and of the operation of such technology, needs to be driven by multidisciplinary teams working together in organizations: technologists with specialist technology, systems, and data expertise, and PAs with deep knowledge of business processes, risks and controls, and a strong code of ethics.[23] Stakeholders observe that for small and medium

---

[22] In a US context, see, for example, commentary about potential liability for enforcement actions in this area by the US Federal Trade Commission in "FTC Issues New Guidance, Warning That Bias in Artificial Intelligence Could Create Potential Liability for Enforcement Actions" (April 24, 2021) National Law Review: https://www.natlawreview.com/article/ftc-issues-new-guidance-warning-bias-artificial-intelligence-could-create-potential

[23] See, for example, Catherine Bannister & Jessica Sierra, "Ethical Technology is a Team Sport" (2021), online Deloitte: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/about-deloitte/us-ethical-technology-is-a-team-sport.pdf; Beena Ammanath, "Thinking Through the Ethics of New Tech…Before There's a Problem" (November 9, 2021) Harvard Business Review: https://hbr.org/2021/11/thinking-through-the-ethics-of-new-techbefore-theres-a-problem; and Karen Hao, "When

enterprises or practitioners (SME/Ps), however, they might not have the resources available to establish multidisciplinary teams, to seek expert advice when relying on or using technology, and to maintain adequate controls over security. This could be problematic and result in systems that are not fit-for-purpose and at-risk of data and other cybersecurity breaches.

Sustainability

34. PAs are viewed as stewards of both financial and non-financial (i.e., environmental, social, and governance (ESG)[24]) information, and are well placed to perform and report on analyses of such information, as well as provide assurance over the reported information.[25]

35. Sustainability is rapidly becoming a core expectation of organizations and is closely tied to ethical stewardship and good governance. Fueling this core expectation, is a major shift in investors' capital allocation to businesses perceived as more sustainable, viewed through an ESG prism.[26] Specifically, sustainable funds are continuing to attract capital at a record pace. For example, in the United States such funds reached $51 billion in 2020 – more than double the total for 2019 and nearly 10 times more than in 2018, according to Morningstar.[27] Investors are now subjecting ESG to the same scrutiny as operational and financial considerations, becoming skeptical of ESG disclosures and commitments, and expecting more litigation as a result of companies not delivering on ESG promises.[28]

36. For meaningful progress in sustainability reporting, there is a need for technology to process the massive volume of data in order to track and narrate such information. Accordingly, considerations to enable the effective application of technology for sustainability reporting include:

    - What data should be measured? Data[29] is integral to how an organization collects, tracks, and reports on sustainability. Furthermore, such data collection and tracking need to be conducted in a timely fashion in order for the reporting to be of value.
    - What is the right set of technology tools to collect and analyze the data? This could include Internet-of-Things devices, cloud computing solutions, AI machine learning, data analytics software tools, etc.

37. It is observed, however, that there remains a relative lack of uptake in new technologies to support sustainability and mitigate climate change because the business case remains less tangible or

---

Algorithms Mess Up, The Nearest Human Gets The Blame" (May 28, 2019) MIT Technology Review: https://www.technologyreview.com/2019/05/28/65748/ai-algorithms-liability-human-blame/

[24] In this regard, stakeholders also commented that the current lack of globally consistent standards, regulations, guidelines, as well as standardized requirements for service providers hampers the ability of PAs to effectively take on this stewardship role for sustainability reporting.

[25] How CPAs can lead ESG Initiatives (January 2021): https://www.cpacanada.ca/en/business-and-accounting-resources/strategy-risk-and-goverance/corporate-governance/publications/esg-and-business-resilience

[26] IESBA's Strategy Survey 2022: Part 1 on "Responding to developments relating to reporting and assurance of sustainability developments"

[27] Center for Audit Quality: Auditors and ESG Information: https://www.thecaq.org/collections/auditors-and-esg/

[28] 2021 Trust Barometer Special Report: Institutional Investors (November 2021): https://www.edelman.com/trust/2021-trust-barometer/investor-trust

[29] World Economic Forum COP26 Live – The number one ESG challenge that organizations face is data (October 2021): https://www.weforum.org/agenda/2021/10/no-1-esg-challenge-data-environmental-social-governance-reporting/

insufficiently understood. There is also a push to understand sustainability information and the underlying drivers of progress. For example, cryptocurrency mining consumes a lot of energy, but whether and how such mining adds value, and how it compares to the energy usage to support traditional financial markets, should be better understood. Further, cryptocurrency transactions[30] and AI applications[31] are also resource intensive. The Working Group believes that PAs are well-positioned to play a role in this analysis space.

B. Technology Landscape

38. This section covers the trends, opportunities, and impact/risks of the following technologies and related issues: RPA, AI, blockchain, cloud computing, and data governance, including cybersecurity. Key ethics-related concerns arising from these technologies and issues are covered in the subsequent subsection entitled *C: Potential Ethics Impact on the Behavior of PAs*. The Working Group notes that most of the ethics-related impact/risks and key concerns are addressed by provisions in the extant Code and proposals in the Technology ED. Those that the Working Group believes can benefit from further guidance are outlined in *Section III. Insights and Recommendations*.

39. Stakeholders report that the most common emerging technologies and technology-related issues currently impacting business processes are RPA, AI (including intelligent process automation (IPA)),[32] cybersecurity (including data privacy), and blockchain. It was consistently reported, however, that the uptake by organizations of AI and blockchain-related technologies is slower than expected and slower relative to the publicity these technologies receive. Based on stakeholder and TEG commentary, as well as desk research, it appears that most organizations are finding these technologies challenging to effectively implement as a result of process fragmentation, resources being allocated to other priorities, difficulties in establishing business cases (for example, a lack of understanding of the return on investment (ROI) arising from the technology or a belief that the ROI is too slow), and the general lack of maturity, and accordingly lack of understanding, of the technologies.

40. Nevertheless, accelerated implementation of transformative technologies has been observed – particularly in the past couple of years, often connected with mitigating business issues related to the COVID-19 pandemic, such as RPA, cloud computing, tools to support remote work and access, and addressing cybersecurity concerns.

Robotic Process Automation

Trends

41. RPA, also known as software robotics (“bots”), uses automation to mimic back-office human tasks and essentially represents digital workers in an organizations’ business unit.

42. Several industries are at the forefront of leveraging RPA technology to streamline their operations, including banking and financial services, insurance, retail, and healthcare.[33] Many major banks, for

---

30 See, for example, Alex Hern, “Waste from one bitcoin transaction ‘like binning two iPhones’ (Sept 2021) The Guardian: https://www.theguardian.com/technology/2021/sep/17/waste-from-one-bitcoin-transaction-like-binning-two-iphones

31 Abhishek Gupta, “Quantifying the Carbon Emissions of Machine Learning” (June 2021) Montreal AI Ethics Institute: https://montrealethics.ai/quantifying-the-carbon-emissions-of-machine-learning/

32 IPA refers to the application of AI (including its sub-fields of computer vision, machine learning, etc.) to RPA.

33 Robotic Process Automation by IBM Cloud Education (October 2020): https://www.ibm.com/cloud/learn/rpa

example, use RPA solutions to automate tasks, such as customer research, account opening, inquiry processing, and tasks aimed at preventing and detecting fraud and money laundering/terrorist financing. Banks typically deploy thousands of bots to automate manual, high-volume data entry and analysis. These processes entail a plethora of tedious, rule-based tasks that automation streamlines.[34]

43. In today's businesses, bots are already performing data entry, generating reports, reading PDF documents and invoices, sending emails, etc. The use of IPA to enable the bot to learn as it processes transactions, remains less common, although such use is on the rise. Consider, for example, the rise of anti-money laundering and anti-terrorism assessments that use AI-enabled automation.[35]

44. Accordingly, demand for roles in areas such as data entry, bookkeeping, and administrative support is decreasing as automation and digitization in the workplace increase.[36] In this regard, it is observed that roles in such areas (e.g., bookkeeping, including the preparation of reconciliations, etc.) tend to be routine or have well-defined steps to follow or are repetitive. For the accounting profession, in particular, there will be wide-ranging impacts, with some estimating that 94% of U.S. accountant and auditor jobs are likely to be impacted by automation.[37] Roles such as strategy formulation, business development, strategic decision support, and risk management are less likely (20% or less) to be automated away in the foreseeable future.[38]

Opportunities

45. Whereas automation does impact some traditional PA roles, it also means that there are new roles created to enable the delivery of activities using technology and opportunities for PAs to undertake some of these less mundane tasks and provide more value-added services. For example, stakeholders observed that PAs are in an ideal position to enable RPA implementation as they have the knowledge of both the business processes and activities being automated, and the governance process risks related to RPA implementation, such as (a) operational, (b) financial, (c) regulatory, (d) organizational, and (e) technological risks.[39] The overall key components to enabling good RPA governance include setting in place appropriate governing bodies and organizational constructs, and

---

34 *Ibid*.

35 JDsupra – AI and Algorithms in Financial Services – Future Areas of Focus (July 2022): https://www.jdsupra.com/legalnews/ai-and-algorithms-in-financial-services-1487837/

36 See, for example, World Economic Forum Future Jobs Survey (October 2020): WEF_Future_of_Jobs_2020.pdf (weforum.org) and New York Times, "The Robots are Coming for Phil in Accounting" (March 6, 2021): https://www.nytimes.com/2021/03/06/business/the-robots-are-coming-for-phil-in-accounting.html

37 *Ibid*.

38 Presentation on Transforming the Finance Function with RPA (November 2021): https://www.ifac.org/system/files/uploads/IESBA/RPA-Transforming-Finance-Function.pdf

39 Operational risks: insufficient exception handling in process workflows or inefficient operational delivery from poor bot resource management. Financial risks: poorly defined requirements for bots leading to financial misstatements or inaccurate payments. Regulatory risks: humans directing bot activities in a fraudulent manager for government reporting. Organizational risks: Inadequate change management, documentation, or business continuity planning. Technological risks: instability of integrating applications and the effect that might have on bot performance, cybersecurity risks, inappropriate access controls

determining the appropriate operational life cycle, internal controls, technology governance, performance management, and vendor management.

46. The Working Group notes that a PA's adherence to the fundamental principles of the Code, and skillset in exercising ethical decision-making (for example, through having an inquiring mind and exercising professional judgement when applying the Code's conceptual framework),[40] help facilitate an effective and ethical RPA implementation. In addition, stakeholders reported that the most successful RPA implementations occur when PAs work closely with IT professionals to advise them on the intricacies of the business processes, the inputs available, the impact desired, and the outputs required from the RPA solution.

Impact/Risks

47. Implementing RPA without fully understanding how its functionality can fit with business needs might result in digital transformations and related internal controls that are not suitable for their intended purpose. Stakeholders noted that when PAs have a good understanding of the capability of RPA, better adapted controls can be implemented and digital transformation through RPA can be enabled more effectively and efficiently. For example, segregation of duties from an internal control perspective becomes less about what the bot has access to, and more about what the human directing the inputs to the bot's activities has access or authority to do. In addition, there are new segregation of duties considerations created around bot creation (i.e., programming what the bots do) versus orchestration (i.e., running the bots).

48. Stakeholders also emphasized consideration of whether there is over-reliance on the RPA and, accordingly, whether there is sufficient, competent human oversight over such automated processes and their outputs. In this regard, the Working Group notes that if a PA is using RPA, the PA might consider the following in determining whether there are threats to compliance with the fundamental principles:

- Is the PA competent to oversee the reasonableness of the output of the technology?
- Is the PA aware of the extent of reliance on the bot (potential automation bias or over-reliance on the technology)?
- Is management taking responsibility for the bot's decisions such as authorizing transactions and whether the task being automated requires little or no professional judgment?

49. In addition, stakeholders pointed out that selecting and prioritizing the right automation opportunity are key for successful RPA implementation. Some questions they suggested a PA might ask when determining whether RPA implementation is appropriate include:

- Is the relevant data readily available, standardized, and of appropriate quality? For example, if the entity has a low level of digitalization, then the error rate might be comparatively higher as paper documents will need to be scanned to enable RPA, which could introduce errors.
- Is the business process highly manual and repetitive?
- Is the process mature, with definable criteria, rule-based with a low exception rate? For example, in automating the accounts payable process, the conditions around payment should be well-defined and documented – including processes over the verification of the vendor,

[40] Section 120 *The Conceptual Framework* of the Code

vendor payment details, validity of the transaction (e.g., goods received match the invoice and purchase order), etc.

- What is the impact of automating the process on the overall control and regulatory environment?
- What value is created by deploying RPA, for example, financial, better staff utilization, or others?
- What are the potential organizational or business unit process implications of automation?[41] For example, impact on human resources, the potential of automating a poorly designed process, or the cascading effects of poor quality data entering the system.

50. Finally, stakeholders also highlighted that another factor to enable successful automation is the importance of appointing a change or transformation officer with a mix of business and technology understanding to document current processes and develop a roadmap for shifting towards automation. However, it was also noted that significant communication gaps between departments (IT and the business function) frequently exist, leading to a lack of understanding and poor specificity of needs and timelines.

Artificial Intelligence

Trends

51. AI combines computer science and robust datasets to enable problem-solving and decision-making capabilities that mimic human intelligence. Today's AI is considered relatively "narrow" or "weak AI," where machines focus on performing specific tasks. Such AI-enabled applications are comparatively commonplace. Examples include digital assistants, natural language question-answering systems, medical imaging analysis tools, statistical and predictive tools, text generating language models, and early-stage autonomous vehicles. AI engineers and scientists are striving for "general AI" or "strong AI," where AI systems are envisioned to have cognitive abilities similar to a human. Whereas these AI systems are still theoretical with no practical examples in use today, AI researchers continue to explore their development.[42]

52. As AI systems continue to grow in sophistication and complexity, there is a significant risk that they will become less explainable as how such systems evaluate data and reach outcomes or decisions becomes more opaque.[43] PwC, amongst many other organizations, observes in a whitepaper on the topic:

---

[41] See also Ashley Nunes, "Automation Doesn't Just Create or Destroy Jobs — It Transforms Them" (November 2, 2021) Harvard Business Review: https://hbr.org/2021/11/automation-doesnt-just-create-or-destroy-jobs-it-transforms-them

[42] Artificial Intelligence by IBM Cloud Education (June 2020) https://www.ibm.com/cloud/learn/what-is-artificial-intelligence and Jeff Dean, "Google Research: Themes from 2021 and Beyond" (January 11, 2022) Google AI Blog: https://ai.googleblog.com/2022/01/google-research-themes-from-2021-and.html

[43] On a related note, a significant qualitative research study involving 602 thought leaders (e.g., technology innovators and developers, business and policy leaders, researchers and activists) found that 68% believed that ethics principles focused primarily on the public good will not be employed in most AI systems by 2030 and will instead continue to be primarily focused on optimizing profits and social control. See Pew Research Center, "Experts Doubt Ethical AI Design Will Be Broadly Adopted as the Norm Within the Next Decade" (June 16, 2021): https://www.pewresearch.org/internet/2021/06/16/experts-doubt-ethical-ai-design-will-be-broadly-adopted-as-the-norm-within-the-next-decade/

> *The central challenge is that many of the AI applications using [machine learning] operate within black boxes, offering little if any discernible insight into how they reach their outcomes. For relatively benign, high volume, decision making applications such as an online retail recommender system, an opaque, yet accurate algorithm is the commercially optimal approach. [...] the use of AI for 'big ticket' risk decisions in the finance sector, diagnostic decisions in healthcare and safety critical systems in autonomous vehicles have brought this issue [knowing if it's an error or a reasonable decision] into sharp relief. With so much at stake, decision [m]aking AI needs to be able to explain itself.*[44]

Therefore, as the whitepaper notes, the more critical a function an AI system performs, the more interpretability (through a combination of transparency and explainability)[45] is required.

Opportunities

53. AI provides opportunities for PAs to leverage their organizational data, by uncovering new relationships through analyzing such data, and increasing efficiencies. For example, data analytics AI software can augment understanding of data relationships and fuel predictive models for financial processes, such as forecasting sales and informing more accurate demand planning (e.g., expected credit loss forecasting in banking and finance). In addition, intelligent drones can be used for inventory and infrastructure management, etc.

54. Specific to audit firms, and in particular larger firms, it is observed that some examples of AI used to enable efficiencies include:[46]

- Using AI to analyze data from non-traditional sources, such as social media, emails, phone calls, public statements from management, etc., to identify potential risks relevant to client acceptance and continuance assessments.
- Using natural language processing and machine learning to analyze both structured and unstructured information, such as global regulatory notices, industry reports, regulatory penalties, news, public forums, etc., to detect relevant audit risks and for fraud detection.

---

[44] PwC, Explainable AI: Driving business value through greater understanding (2018): https://www.pwc.co.uk/audit-assurance/assets/explainable-ai.pdf

See also, for example:

- Deloitte, "Unleashing the power of machine learning models in banking through explainable artificial intelligence" (May 2022): https://www2.deloitte.com/us/en/insights/industry/financial-services/explainable-ai-in-banking.html
- KPMG, Controlling AI: The imperative for transparency and explainability (June 2019): https://advisory.kpmg.us/articles/2019/controlling-ai.html
- World Economic Forum, Guidelines for AI Procurement (September 2019): https://www3.weforum.org/docs/WEF_Guidelines_for_AI_Procurement.pdf
- Canadian Public Accountability Board, *Technology in the Audit* (August 2021) CPAB Exchange: https://cpab-ccrc.ca/docs/default-source/thought-leadership-publications/2021-technology-audit-en.pdf

[45] Christian Herzog, "On the Risk of Confusing Interpretability with Explicability" (2022) AI and Ethics 2:219-225, online: https://link.springer.com/article/10.1007/s43681-021-00121-9

[46] IAASB Digital Technology Market Scan: Artificial Intelligence—A Primer (March 2022): https://www.iaasb.org/news-events/2022-03/iaasb-digital-technology-market-scan-artificial-intelligence-primer

- AI tools, benefiting from increases in the quality and quantity of available "training" data (i.e., data that the system uses to learn), applied to data sets to algorithmically identify outliers and anomalous data and to perform predictive analytics for use in areas such as testing large transaction populations, auditing accounting estimates, and going concern assessments.
- Document processing, review, and analysis by using optical character recognition to identify and extract key details from contracts (e.g., leases) and other documents (e.g., invoices).
- Inventory and physical asset verification procedures through use of intelligent drones with computer vision (image recognition), particularly for larger capital assets, such as trucks, utility infrastructure, or the inspection of large-scale business sites, such as tree farms.
- AI technologies to support auditors' work on financial statement disclosures, enabling easier identification of missing disclosure requirements and non-compliance.

55. In general, AI models need data to train on, and training on actual client and customer data is the most effective and efficient. As a result, it is becoming more common for firms and companies to want to use such "real" data to train their AI models to enhance audit quality or business insights. This is seen by firm stakeholders to be akin to PAs of the past taking the "lessons learned" from prior engagements or projects and applying them to their next project or task, except that now the "lessons learned" are applied by the AI model instead. It was noted that along with the benefits of improving the quality of the AI model's outputs, using such "real" training data comes with risks to cybersecurity, confidentiality and privacy, as well as potential threats to independence. See discussion on *Focus on Data Governance*.

56. AI systems and AI-based applications are also becoming increasingly important as tools to monitor other technology systems, including other AI systems, because more traditional methods of monitoring are unable to maintain the frequency of evaluation needed. Examples include the need for continuous monitoring in some cybersecurity environments mitigating threats from sophisticated actors, as well as helping to validate AI models in search of bias or other vulnerabilities as organizations strive for ethical AI.[47]

Impact/Risks

57. There is often an assumption that AI technology is neutral, but the reality is far from it.[48] AI algorithms are created by humans, and humans have inherent and unconscious biases.[49] Therefore, AI is never fully objective and instead reflects the world view of those who built the systems, as well as the data ingested by the system.[50] Stakeholders observed that inherent bias in data is the biggest issue with

---

47 See, for example, Deloitte, "Deloitte AI Institute Team With Chatterbox Labs to Ensure Ethical Application of AI" (March 15, 2021): https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-ai-institute-teams-with-chatterbox-labs-to-ensure-ethical-application-of-ai.html

48 See, for example, Karen Hao, "The true dangers of AI are closer than we think" (October 21, 2020) MIT Technology Review: https://www.technologyreview.com/2020/10/21/1009492/william-isaac-deepmind-dangers-of-ai/

49 See, for example, Gabbrielle M Johnson, "Algorithmic Bias: On the Implicit Biases of Social Technology" (2021) Synthese 198(1), doi: 10.1007/s11229-020-02696-y, online: http://philsci-archive.pitt.edu/17169/1/Algorithmic%20Bias.pdf

50 HBR: AI Fairness Isn't Just an Ethical Issue (October 2020) https://hbr.org/2020/10/ai-fairness-isnt-just-an-ethical-issue

AI, and that such bias might not be fully mitigated in the programming, and attempts to correct bias might actually introduce new bias.

58. Bias can creep into algorithms in several ways. AI systems learn to make decisions based on both training data and testing data,[51] which can include biased human decisions or reflect historical or social inequities, even if sensitive variables such as gender, race, and sexual orientation have been removed. Data sampling is also a source of bias, in which groups are over- or under-represented in the data set.[52] Stakeholders commented that PAs need to be aware of the extent to which bias is impacting the outputs of technology, and to ensure that they have the appropriate mindset, competence, and tools to do this.

59. Understanding the technology and having regard to the purpose for which it is to be used are also key to assessing whether the output of technology is reasonable. In this regard, stakeholders also highlighted that PAs need to be aware that the approach to AI learning might also affect its risk profile for producing accurate and reliable outputs.[53] Furthermore, understanding how data was made available for training and testing the AI system – and how confidentiality, including data privacy, has been considered and maintained – is also important.

60. This illustrates the importance of building ethical AI, in respect of which there are many parallel initiatives around the world (around 200 sets of AI ethics guidelines have been developed by various governments, multilateral organizations, non-governmental organizations, and corporations).[54] Importantly, in November 2021, UNESCO's General Conference of 193 member states adopted the

---

[51] Training data is the information used to train an algorithm for a specific output. Training data contains both the anticipated output as well as the input data in order to get the algorithm's desired output to run smoothly. Testing data is a dataset that is used to assess how well the model performs when making forecasts on it. Testing data contains only the input data, not the anticipated result. The algorithm's output is then compared to the "actual" result to assess how well the algorithm was trained.

[52] HBR: What do we do about biases in AI? (October 2019) https://hbr.org/2019/10/what-do-we-do-about-the-biases-in-ai

[53] AI can learn through supervised or unsupervised learning. Supervised learning uses labelled (i.e., preprocessed data which has been labelled for a specific context) datasets to train the AI to classify data or predict outcomes accurately with human intervention. Unsupervised learning uses unlabeled (i.e., raw data straight from the source) datasets to discover "hidden" patterns in data without human intervention. Classifying big data can be a real challenge in supervised learning, but the results are highly accurate and trustworthy. In contrast, unsupervised learning can handle large volumes of data in real time, but there is a lack of transparency into how data is clustered and a higher risk of inaccurate results. (IBM Education, August 2020: Supervised vs. Unsupervised Learning: What's the Difference? | IBM)

[54] See, for example:

- AlgorithmWatch, "AI Ethics Guidelines Global Inventory" (accessed July 9, 2022): https://inventory.algorithmwatch.org
- Montreal AI Ethics Institute, "AI Ethics in the Public, Private, and NGO Sectors: A Review of a Global Document Collection" (April 12, 2001): https://montrealethics.ai/ai-ethics-in-the-public-private-and-ngo-sectors-a-review-of-a-global-document-collection/
- PwC, "10 Ethical AI principles the world (mostly) agrees on — and what to do about them" (August 2021): https://www.pwc.com/us/en/tech-effect/ai-analytics/how-to-make-ai-ethical.html

Guideline examples include: U.S. Government Accountability Office's Accountability Framework for Federal Agencies and Other Entities, the Institute of Electrical and Electronics Engineers' (IEEE) Ethically Aligned Design, the Committee of Sponsoring Organizations of the Treadway Commission (COSO)'s Applying the COSO Framework and Principles to Help Implement and Scale Artificial Intelligence.

Recommendation on the Ethics of AI, which is the first truly global standard-setting instrument on AI ethics.[55]

61. Stakeholders observed that building or ensuring ethical AI systems includes understanding the data going into the model, how the model operates, and the potential unintended consequences of operating the model. PAs cannot be expected to be the "expert" in technology and fully understand what is "under the hood," but in order to rely on a system, PAs must be comfortable that the output from the technology is reasonable. Given the challenges of some AI systems lacking transparency and explainability, this might not always be possible. In many cases, however, the PA's reliance on the system can be enhanced through gaining an understanding of the controls around the inputs to the system (i.e., quality of the data, including being proactive to understand the inherent biases within the dataset); the system, application, and other general IT controls, such as monitoring the operation of the system or making changes; as well as controls over the analysis of the output. This means that although the PA might not understand the "black box," they can at least be comfortable with the inputs and the control structure monitoring the system and its output in order to reasonably rely on the technology. It is also imperative that for systems supporting decisions with significant consequences, the PA has access to one or more experts who can answer both "how does the system work?" and "why did the system do what it did?".[56]

62. In addition, stakeholders commented that having the ability and competence to ask the "right" questions so that appropriate and fit-for-purpose AI is procured or developed is important. This can be achieved by the PA keeping current and educating themselves on relevant practical guidance and "best practices" specific to their role. Examples include the World Economic Forum's "toolkits" for C-suite executives[57] and Board of Directors.[58]

63. Stakeholders stress that building or ensuring ethical AI systems also involves utilizing a "human in the loop" approach to ensure human expert oversight of, and accountability for, the system. For example, the volume of data inputs and inherent complexity that drive machine learning can create a scenario where the system lacks transparency and explainability, and the impact of bias potentially also goes undetected. Regular monitoring and feedback of any developments or changes in the AI outputs and consulting with experts might help the PA assess the ongoing reasonableness of such outputs. In this regard, the Working Group notes that the Code's requirement for a PA to have an inquiring mind when applying the conceptual framework will help a PA challenge the system to test how it responds across a wide range of stimuli, notwithstanding any conditions, policies and procedures that might be established by the employing organization or firm to address the system's accountability.

64. Ensuring an ethical organizational culture is also core to fostering a safe environment for data scientists and others to escalate concerns over any bias or discrimination identified in AI systems or

---

[55] UNESCO, Recommendation on the Ethics of Artificial Intelligence (November 2021): https://www.unesco.org/en/artificial-intelligence/recommendation-ethics

[56] *Supra* note 44; see also an interesting example of OpenAI's GPT-3 platform being used to explain the purpose of specific computer in Simon Willison, "Using GPT-3 to Explain How Code Works" (July 9, 2022) Simon Willison blog: https://simonwillison.net/2022/Jul/9/gpt-3-explain-code/

[57] World Economic Forum's "Empowering AI Leadership: AI C-Suite Toolkit" (January 2022): Empowering AI Leadership: AI C-Suite Toolkit | World Economic Forum (weforum.org)

[58] World Economic Forum's "Empowering AI Leadership - An Oversight Toolkit for Boards of Directors" (2022): https://express.adobe.com/page/RsXNkZANwMLEf/

data without the fear of retaliation. For example, the former co-lead of Google's Ethical AI team has alleged that she was fired over a dispute in relation to a research paper she co-authored opining that technology companies could do more to stop AI systems designed to mimic human writing and speech from exacerbating historical gender biases and using offensive language.[59] The Working Group notes that PAs are expected to encourage and promote an ethics-based culture within their organizations, taking into account their position and seniority in the organization. This role is key and becoming even more important in the face of transformational technology.

65. Against this backdrop, the importance of regulating AI systems is also being increasingly recognized by governments around the world.[60] For example, the European Commission has proposed a risk-based approach to regulating AI systems, whereby such systems are rated on a scale ranging from "minimal or no risk" to "unacceptable risk."[61] Under this approach, AI systems providing social scoring of humans are classified as being of unacceptable risk and are prohibited, whereas AI enabling recruitment and medical services are of high risk and are only permitted subject to compliance with certain additional requirements.

Blockchain (Including Cryptocurrencies, Tokens and Decentralized Finance)

Trends

66. In its basic form, blockchain is a decentralized digital ledger, and has been touted as having the potential to revolutionize the operations of businesses, governments, and economies, specifically in the way transactions are initiated, processed, authorized, recorded, and reported. Such changes in business models and business processes will impact back-office activities such as financial and non-financial reporting and tax preparation.

67. Stakeholders reported mixed views over whether blockchain can and will replace the financial reporting systems and activities of today. It was reported that organizations still see blockchain as an additional investment that ultimately does not function any differently from other enterprise resource planning (ERP) systems currently in use. In many instances, parallel systems continue to be run to ensure the data on the blockchain is accurate. Further, significant resources are being spent reconciling the blockchain data with more traditional systems in proof-of-concept trials, despite the promise that blockchain will remove the need for traditional approaches. As such, blockchain has not yet reduced the burden of organizational recordkeeping in most organizations. For mass uptake, other parties along the supply chain need to see the appeal of accessing the blockchain, have an

---

[59] The Guardian "More than 1,200 Google workers condemn firing of AI scientist Timnit Gebru" (December 2020): https://www.theguardian.com/technology/2020/dec/04/timnit-gebru-google-ai-fired-diversity-ethics

[60] There are indications that increased government regulation is supported by knowledgeable business leaders. For example, a 2021 KPMG US study found that "business leaders are conscious that controls are needed and overwhelmingly believe the government has a role to play in regulating AI technology…Business leaders with high AI knowledge (92 percent) are more likely to say the government should be involved in regulating AI technology in comparison to total business leaders (87 percent)." See KPMG, *Thriving in an AI World* (April 2021): https://info.kpmg.us/content/dam/info/en/news-perspectives/pdf/2021/Updated%204.15.21%20-%20Thriving%20in%20an%20AI%20world.pdf

[61] European Commission's proposed artificial intelligence act (April 2021): The Act | The Artificial Intelligence Act; Melissa Heikkilä, "A quick guide to the most important AI law you've never heard of" (May 13, 2022) MIT Technology Review: https://www.technologyreview.com/2022/05/13/1052223/guide-ai-act-europe/

extent of trust and knowledge about blockchain systems, and agree with the value proposition it provides.

68. Nevertheless, emerging applications across finance, business, government, and healthcare are growing.[62] Such applications combine blockchain technology with the use of smart contracts (i.e., digital versions of the standard paper contract that automatically verify fulfillment and enforce and perform the terms of the contract).[63] From an industry perspective, banking leads the way in blockchain spending, accounting for nearly 30% of the worldwide total in 2021.[64] The next largest industries for blockchain spending are process manufacturing and discrete manufacturing, which together account for more than 20% of worldwide spending.[65]

Cryptocurrencies, Tokens, and Decentralized Finance

69. Cryptocurrencies, such as Bitcoin and Ethereum, run on blockchain technology and are seen as a potential tool to promote and accelerate financial inclusion by providing those people who do not have access to traditional financial institutions with an alternative means of transferring funds.[66] The value of cryptocurrencies, however, remains extremely volatile and the related crypto-mining that comes with it brings enormous environmental cost.[67] This has led several governments, such as China, to restrict cryptocurrency trading and/or mining.[68]

70. Decentralized finance ("DeFi") is an umbrella term for financial services on public blockchains, primarily Ethereum, which do not require paperwork or a third party. Essentially, it creates an entire digital alternative to traditional financial markets, but without the associated costs (i.e., office towers, trading floors, banker salaries). This is being advocated as having the potential to create more open, free, and fair financial markets that are accessible to anyone with an internet connection.[69]

71. Unfortunately, as cryptocurrency advertises a combination of anonymity, ease of use, and the ability to circumvent international borders and regulations, it has also become the preferred currency for

---

62 Business Insider: What growing list of applications and use cases of blockchain technology in business and life (February 2022): https://www.businessinsider.com/blockchain-technology-applications-use-cases

63 Corporate Finance Institute: Smart Contract: Smart Contract - Overview, How It Works, Role in Blockchain Tech (corporatefinanceinstitute.com); Chi-Chun Chou, Nen-Chen Richard Hwang, Gary P Schneider, et al, "Using Smart Contracts to Establish Decentralized Accounting Contracts: An Example of Revenue Recognition" (2021) Journal of Information Systems 35(3):17-52, online: https://doi.org/10.2308/ISYS-19-009

64 IDC "Global Spending on Blockchain Solutions Forecast to be Nearly $19 Billion in 2024" (April 2021): https://www.idc.com/getdoc.jsp?containerId=prUS47617821

65 *Ibid.*

66 Close to a third of the world's adults are "unbanked," and the problem is not limited to the developing world. While mobile adoption is supporting financial inclusion globally, increased cryptocurrency adoption is also improving financial inclusion, as well as helping to grow wealth and safeguard assets. – World Economic Forum "Cryptocurrencies are democratizing the financial world" (January 2021): https://www.weforum.org/agenda/2021/01/cryptocurrencies-are-democratising-the-financial-world-heres-how/

67 Business Insider "What are the environmental impacts of cryptocurrencies?" (March 2022): https://www.businessinsider.com/personal-finance/cryptocurrency-environmental-impact

68 Euronews "These are the countries where crypto is restricted or illegal" (January 2022): https://www.euronews.com/next/2022/01/11/bitcoin-ban-these-are-the-countries-where-crypto-is-restricted-or-illegal2

69 Coinbase "What is DeFi?": What is DeFi? | Coinbase

purchasing illicit goods and the demanded payment form in most ransomware attacks.[70] DeFi similarly also creates risks for money laundering and terrorist financing due to its technologically dynamic nature and evolving regulation[71] and anonymity of users. Note, however, that the anonymity of cryptocurrencies is not absolute, as immutable transaction trails are created, which allow law enforcement agencies using forensic techniques to track criminals, such as ransomware attackers (e.g., the Colonial Pipeline attack in the U.S.)[72] and child sex abuse traffickers.[73]

72. Despite the volatility and associated risks, businesses are increasingly accepting cryptocurrencies as a form of payment[74] and hold cryptocurrencies as investments or for trade on their balance sheets. In addition, there are governments looking to adopt cryptocurrency as legal tender, with El Salvador being the first country to embrace a cryptocurrency (Bitcoin) as legal tender in 2021.[75]

73. Separately, but related, the development of central bank digital currency (CBDC) – virtual money backed and issued by a central bank – is being explored or has been launched by a variety of governments including the United States, United Kingdom,[76] India,[77] China,[78] Nigeria, and the Bahamas. CBDCs are anticipated to enable individuals and businesses to send instant payments

---

70 BakerTilly "Cryptocurrency and money laundering" (November 2021): https://www.bakertilly.com/insights/cryptocurrency-and-money-laundering; Kate Rooney, "Overall bitcoin-related crime fell last year, but one type of crypto hack is booming" (January 2021) CNBC: https://www.cnbc.com/2021/01/24/overall-bitcoin-related-crime-fell-last-year-but-one-type-of-crypto-hack-is-booming.html; Corin Faife, "NFT money laundering is a small but growing sector, says Chainalysis report" (February 2022) Verge: https://www.theverge.com/2022/2/2/22914056/nft-money-laundering-chainalysis; Carly Page & Anita Ramaswamy, "US Treasury sanctions Tornado Cash, accused of laundering stolen crypto" (August 2022) TechCrunch: https://techcrunch.com/2022/08/08/treasury-tornado-cash-laundering-stolen-crypto/

71 The virtual asset sector is fast-moving and technologically dynamic, which means continued monitoring and engagement between the public and private sectors is necessary. In October 2021, the Financial Action Task Force (on Money Laundering) (FATF) updated its 2019 Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (VASPs): 2019 Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers (VASPs). This updated Guidance issued in October 2021 forms part of the FATF's ongoing monitoring of the virtual assets and VASP sector. Countries are also responding to these threats. See, for example, Naomi O'Leary, "EU to ban cryptocurrency anonymity in anti-money laundering plan" (July 2021) Irish Times: https://www.irishtimes.com/business/economy/eu-to-ban-cryptocurrency-anonymity-in-anti-money-laundering-plan-1.4626129

72 Thomson Reuters, "Recovery of Colonial Pipeline ransom funds highlights traceability of cryptocurrency, experts say" (June 2021): https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/colonial-pipeline-ransom-funds/ and Andy Greenberg, "The Colonial Pipeline Hack is a New Extreme for Ransomware" (May 8, 2021) Wired: https://www.wired.com/story/colonial-pipeline-ransomware-attack/

73 Wired, "The Crypto Trap: Inside the Bitcoin Bust That Took Down the Web's Biggest Child Abuse Site" (April 2022): https://www.wired.com/story/tracers-in-the-dark-welcome-to-video-crypto-anonymity-myth/

74 Small Business Trends: Who Accepts Bitcoin as Payment? (March 2022): https://smallbiztrends.com/2021/12/who-accepts-bitcoin.html

75 See, for example, NPR, "El Salvador Just Became The First Country To Accept Bitcoin As Legal Tender" (September 2021): https://www.npr.org/2021/09/07/1034838909/bitcoin-el-salvador-legal-tender-official-currency-cryptocurrency and Bloomberg, "El Salvador's Bitcoin Bet Is Working, Finance Minister Says" (July 28, 2022): https://www.bloomberg.com/news/articles/2022-07-28/el-salvador-s-bitcoin-bet-is-working-finance-minister-says.

76 Saqib Shah, "The UK is considering starting a digital currency" (April 2021) engadget: https://www.engadget.com/uk-considering-starting-digital-currency-123546776.html

77 Amitoj Singh, "India Edges Toward Crypto Legalization With 30% Tax, Announces Digital Rupee" (June 2022) Coindesk: https://www.coindesk.com/policy/2022/02/01/india-to-levy-30-tax-on-crypto-income-cbdc-launch-in-2022-23/

78 James T Areddy, "China Creates Its Own Digital Currency, a First for Major Economy" (April 2021) Wall Street Journal: https://www.wsj.com/articles/china-creates-its-own-digital-currency-a-first-for-major-economy-11617634118

through their depository institution accounts at much higher transactions speeds as compared to traditional transactions (i.e., through Visa, Alipay, etc.) or cryptocurrencies (i.e., Bitcoin).

74. Finally, blockchain applications include the tokenization of physical or digital assets. These blockchain tokens represent the right to a physical or digital asset, for example, a property right on a luxury good, a share in a company, the fractional ownership of a building or property, or a digital artwork. Investors are increasingly trading and investing in such tokens. There are two distinct types of tokens:

- Fungible tokens: Store value and are divisible and non-unique. They can also be:

  (a) Utility tokens, which give holders access to products and services that are blockchain-based, such as cryptocurrency; or

  (b) Security tokens, which represent traditional assets like stocks and shares.

  Furthermore, security tokens can be "listed", i.e., security token offerings (STOs), which is a type of public offering in which security tokens are sold on security token exchanges or cryptocurrency exchanges.

  STOs are more susceptible to regulation than initial coin offerings (ICOs), as ICO tokens offer cryptocurrency digital coins, which are often classified as utility tokens.

- Nonfungible tokens: Store data and represent one unique and indivisible item — physical or intangible — like a picture or intellectual property.

Opportunities

75. Stakeholder outreach has indicated that there are many proof-of-concept projects being tested for blockchain technology use, in particular for governmental and public sector organizations. Such proof-of-concepts are broad, for example, to ensure validity in relation to academic and other credentials, land ownership, reputational history, and vaccine distribution.

76. Within businesses, use cases include supply chain tracking to increase transparency through verification against product counterfeiting and providing participants end-to-end, real time visibility on the movement and source of goods.[79] Examples include:

- Moving meat, including tracking the health status of animals, storage temperature, and even emissions, from the ranch all the way to the consumer;
- Transporting containers and rail cars from port of origin to final destination; and
- Supporting "know your client" processes by setting up new financial accounts more quickly through faster identity verification and providing anti-money laundering audit trails for transactions.

[79] This might also help support ESG reporting through collection and recording of verifiable non-financial data and supply chain transparency (April 2022): Blockchain and Environmental, Social, and Governance Investing (natlawreview.com)

77. Looking ahead in the short-term, industry adoption is expected to increase as there are numerous pilots ongoing in various jurisdictions, and as many large corporations and organizations form consortia to create blockchain ecosystems.[80]

Impact/Risks

78. Stakeholders indicated that when using or implementing blockchain technology, PAs should understand how it works and how other users will access and use the information on the blockchain. For example, do other users have access to only their own information or to all the other elements on the blockchain? Such understanding helps facilitate implementing appropriate data security and privacy protocols to maintain the integrity and confidentiality of the blockchain.

79. Stakeholders questioned how the role of the auditor and auditor independence issues will evolve as the use of blockchain becomes more commonplace. For example, a blockchain-enabled solution developed and implemented by a firm for a client (i.e., for product traceability, such as tracking of products from source to destination) might have participants that are the firm's audit clients. It was highlighted that, among other potential independence considerations, firms should not build the application programming interface (API) to connect its audit client onto a blockchain that it developed or implemented. This is because building the API requires ensuring that the information being "pushed" onto the chain (to write a record, which in this case would be from an audit client) is accurate and suitable for purpose, which might have independence implications. Furthermore, it was questioned whether such blockchain solution would impact the audit client's financial reporting and related internal controls.

80. Specifically with respect to the audit of blockchains, stakeholders stressed that it is important for auditors to understand who all the participants on the blockchain are, as there might be business relationships and professional services provided to these other participants that could raise auditor independence issues. Such understanding might include, for example:

    - Who the other participants on the blockchain are (i.e., recognizing that while this is possible for alliance (i.e., "closed") blockchains, this might not be possible for fully "open" or public blockchain ecosystems);
    - How participants benefit from the blockchain solution;
    - Whether participants will rely on the information in the blockchain for their respective financial and/or non-financial reporting; and
    - Whether the blockchain is closed (private) or open (public). In this regard, it was noted that in all blockchain ecosystems, information on the blockchain is open to all participants. Hence, if an audit firm has access to a blockchain, then technically it is able to view all transactions on that chain, not just those belonging to its clients. Therefore, understanding whether there are conflicts of interest amongst those who might have access is important.[81]

    Stakeholders also noted that if the implementation and uptake of blockchain and smart contracts by companies transform the business ecosystem enough in the future, the auditor's role is also expected

[80] See, for example, Hyperledger: https://www.hyperledger.org, South African Financial Blockchain Consortium: https://www.safbc.co.za, and IBM Food Trust: https://www.ibm.com/blockchain/solutions/food-trust

[81] Katie Bakarich and Jack Castonguay, "Use of Blockchain in Corporate and Financial Reporting and Regulatory Implications" (June 2021): https://www.ifac.org/system/files/uploads/IESBA/06.09-IESBA-Blockchain-Bakarich-Castonguay.pdf

to change and evolve. In addition, relevant upskilling will need to take place to audit blockchains and smart contracts. Where the requisite skills are lacking at this time, firms might rely on technology experts to gain comfort over the technologies applied. It was, however, noted that the technology experts available to rely on are a niche pool and likely be the established technology companies that also develop these tools, leading to potential conflicts of interest. Additionally, it was observed that the lack of requisite skills or standardized audit methodology policies might result in inadequate auditing processes.

81. In terms of potential auditor independence issues in relation to firm staff investing in digital assets issued by audit clients, stakeholders observed that this situation is nothing "new." Stakeholders see it akin to firm staff investing in an audit client's securities, which is prohibited.[82] However, it was also observed that some digital assets might not be classified as "securities" as many token issuers specifically state that their tokens are "utility tokens" and not "securities tokens." As such, in the absence of specific independence guidelines addressing the holding of tokens or similar instruments issued by audit clients, firms might fall back on the measures that safeguard against potential conflicts of interest[83] situations, such as avoiding any transactions when the firm is providing a service (audit or non-audit services) to a token-issuing entity. Ultimately, PAs are required to comply with the Code's fundamental principles, including objectivity and professional competence and due care, and for PAPPs, the requirements for independence[84] in fact and in appearance (which are linked to the fundamental principles of objectivity and integrity).

82. Finally, it is observed that accounting for, disclosure, and regulation of cryptocurrencies is an evolving area creating dynamic complexity for PAs who need to keep up to date with this changing landscape. For example, the:

    (a) IFRS Interpretations Committee discussed and concluded in June 2019 how IFRS Standards should apply to holdings of cryptocurrencies.[85] However, at the IFRS Foundation's June 2022 Conference, it was highlighted that there would be a future project to revisit IAS 38 *Intangible Assets*, which might address cryptocurrencies, among other items.[86]

    (b) IOSCO issued a roadmap in July 2022 to outline workstreams to explore market integrity, investor protection and financial stability risks with respect to crypto and digital assets and decentralized finance.[87]

---

82 Section 510 *Financial Interests* of the Code

83 Section 310 *Conflicts of Interest* of the Code

84 Paragraph 120.15 A1 of the Code

85 IAS 2 *Inventories* or IAS 38 *Intangibles Assets* apply, depending on the facts and circumstances of the holdings – IFRS Interpretations Committee IFRIC Update (June 2019): https://www.ifrs.org/news-and-events/updates/ifric/2019/ifric-update-june-2019/#8

86 More recently, the IASB Chair reiterated at the IFRS Foundation's June 2022 Conference that the June 2021 IFRS interpretation on accounting for crypto currencies continues to apply – IFRS Foundation Conference, IASB Chair Andreas Barckow's Keynote Speech (June 2022): https://www.ifrs.org/news-and-events/news/2022/06/andreas-barckow-ifrs-foundation-conference-keynote-speech/

87 IOSCO Crypto-Asset Roadmap for 2022-2023 (July 2022): OR03/22 Crypto-Asset Roadmap for 2022-2023 (iosco.org)

(c) EU Parliament has agreed on draft rules on supervision, consumer protection, and environmental sustainability of crypto assets.[88]

(d) U.S. SEC has issued a Staff Accounting Bulletin on Accounting for Obligations to Safeguard Crypto-Assets an Entity Holds for its Platform Users.[89]

(e) U.S. FASB has launched a research project on accounting for, and disclosing of, a subset of exchange-traded digital assets and commodities.[90]

(f) AICPA has a practice aid on accounting for and auditing of digital assets.[91]

Cloud Computing

Trends

83. Given exponential data growth,[92] cloud computing is becoming a necessity. There is an increasing use of third-party cloud services such as governance, risk management, and compliance (GRC) and audit management tools for organizations to manage and document their controls. In particular, the COVID-19 pandemic ushered in a new era of cloud-based Software as a Service (SaaS – software distribution models in which a cloud provider hosts applications and makes them available to end users over the internet). In this model, an independent software vendor may contract a third-party cloud provider to host the application or alternatively, with larger organizations, the cloud provider might also be the software vendor.[93]

Opportunities

84. Cloud computing marks a significant shift from the traditional way businesses think about IT resources.[94] One of the biggest impacts is in relation to cost and scalability. Use of cloud eliminates the capital expense of buying, operating, and maintaining local hardware and software and setting up and running on-site datacenters. At the same time, it enables more rapid scaling by changing the service agreement for IT resources with the vendor as needed (i.e., more or less computing power, storage, bandwidth). In addition, cloud computing makes data backup, disaster recovery, and

---

88 European Parliament Press Release (March 2022): https://www.europarl.europa.eu/news/en/press-room/20220309IPR25162/cryptocurrencies-in-the-eu-new-rules-to-boost-benefits-and-curb-threats

89 US SEC (April 2022): SEC.gov | Staff Accounting Bulletin No. 121

90 US FASB Research Projects: https://www.fasb.org/Page/ProjectPage?metadata=FASB_OBJECTIVESOFRESEARCHPROJECTS_022820221200#btnTitle_1

91 AICPA Practice Aid (Q1 2022): https://www.aicpa.org/resources/download/accounting-for-and-auditing-of-digital-assets-practice-aid-pdf

92 Deloitte, "Data: a small four-letter word which has grown exponentially to such a big value": https://www2.deloitte.com/cy/en/pages/technology/articles/data-grown-big-value.html

93 TechTarget "Software as a Service (SaaS)": https://www.techtarget.com/searchcloudcomputing/definition/Software-as-a-Service

94 Microsoft has produced a concise and easy to understand guide to the key benefits, types, and service types of cloud computing, including SaaS. See "What is cloud computing? A beginner's guide" at https://azure.microsoft.com/en-ca/resources/cloud-computing-dictionary/what-is-cloud-computing/

business continuity easier and less expensive because data can be mirrored at multiple redundant sites on the cloud provider's network.

Impact/Risks

85. Stakeholders observed that whether a firm or company decides to use a cloud provider typically involves the following considerations:

    - Security concerns, given the sensitivity of data being processed and stored outside of the organization's direct control (potential market sensitive data, private employee and client data, industry-specific considerations, etc.).
    - Legal, regulatory, and/or professional compliance requirements, such as data sovereignty laws that require data to remain within a particular jurisdiction.

86. Many organizations or firms already use the cloud for their data and accounting systems. When a cloud provider is used, the provider stores data and information related to the particular organization or firm and/or its clients or customers. Hence, the organization or firm must ensure that the provider implements necessary security measures. Designing and implementing an appropriate data governance and management framework that might not have traditionally existed has become a priority, especially in the face of increasing, and ever more sophisticated, cyberattacks. It was noted that this might be particularly challenging for small- and medium-sized entities and practitioners who potentially lack the budget, resources, and negotiating influence needed to engage cloud service providers.

87. Stakeholders indicated that it is challenging to keep up with the direction of evolving data privacy and cybersecurity regulations and best practices. Other important pain points to watch in data governance are: (a) data collection, including the quality of metadata management, (b) data access and controls, and (c) objectivity in data analytics. See discussion on *Focus on Data Governance*.

88. For firms in particular, providing cloud-based services has raised questions over when holding client information and data constitutes "hosting" by a firm, and whether this is permissible or is seen to be assuming a management responsibility. See discussion on *Independence*.

Other Technologies and Technology-related Areas

89. This section highlights other technologies[95] that the Working Group encountered at a high-level during its fact-finding:

[95] See, for example: World Economic Forum "17 ways technology could change the world by 2025" (June 2020): https://www.weforum.org/agenda/2020/06/17-predictions-for-our-world-in-2025/; Institute of Electrical and Electronic Engineers (IEEE) Computer Society "Technology Predictions" (2022): https://ieeecs-media.computer.org/media/tech-news/tech-predictions-report-2022.pdf; EY, "Five major trends which will underpin another decade of digital innovation" (March 25, 2021): https://www.ey.com/en_gl/consulting/five-major-trends-which-will-underpin-another-decade-of-digital-innovation; Deloitte, "Tech Trends 2022" (2022): https://www2.deloitte.com/content/dam/insights/articles/US164706_Tech-trends-2022/DI_Tech-trends-2022.pdf

Maturity[96]	Technology	Opportunities	Impact/Risks
	Synthetic media: Recordings or live presentations (video or audio) that use AI to create "fake" content or "deepfakes"	• Use of deepfake "artificial reality identities" to connect with clients and make presentations[97] • Training simulations for education and evaluation • Reaching and engaging with larger, more diverse audiences in an efficient way • Opportunity for NFTs as it can facilitate determining the authenticity of a physical or digital asset (i.e., virtual/digital content such as photos, videos, audio, or tweets) because the original source of such videos will be tagged in	• Prevalence of mis-/disinformation[99] to shift public opinion in spite of factual and evidence-based information to the contrary, and resulting challenges in undoing viral social media posts that present such information • Use of deepfakes to commit fraud, for example, consider a deepfake of a senior executive at a company or an audit partner commenting on sensitive information circulating around social media[100] • Identity theft poses a threat to authorization processes • Increased need for being alert and applying

[96] **Green**: Already here; **Orange**: On the horizon, i.e., emerging; **Brown**: Nascent, i.e., still largely theoretical and under development

[97] Tom Simonite, "Deepfakes are now making business pitches" (August 2021) Wired: https://www.wired.com/story/deepfakes-making-business-pitches; James Vincent, "Deepfake dubs could help translate film and TV without losing an actor's original performance" (May 18, 2021) Verge: https://www.theverge.com/2021/5/18/22430340/deepfake-dubs-dubbing-film-tv-flawless-startup; Christa Lesté-Lasserre, "Fake faces created by AI look more trustworthy than real people" (February 14, 2022) New Scientist: https://www.newscientist.com/article/2308312-fake-faces-created-by-ai-look-more-trustworthy-than-real-people/

[99] See, for example, Matt Murphy, "The Dawn of AI Mischief Models" (August 3, 2022) Future Tense, online Slate: https://slate.com/technology/2022/08/4chan-ai-open-source-trolling.html. Note that on other side of the equation, Microsoft has developed a tool, Video Authenticator that can analyze a still photo or video to provide confidence score that the medium has been artificially manipulated – Microsoft Press Release (September 2020): https://blogs.microsoft.com/on-the-issues/2020/09/01/disinformation-deepfakes-newsguard-video-authenticator/

In addition, Microsoft, the BBC, CBC/Radio-Canada, and the New York Times have launched Project Origin to use such Microsoft technology for publishing tamper-proof metadata – TechRepublic "Microsoft and others in big tech are working to bring authenticity to videos, photos" (July 2021): https://www.techrepublic.com/article/deepfakes-microsoft-and-others-in-big-tech-are-working-to-bring-authenticity-to-videos-photos/

[100] See, for example, the 5 commerce scenarios presented in US Department of Homeland Security, *Increasing Threats of Deepfake Identities* (2021): https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf

Maturity[96]	Technology	Opportunities	Impact/Risks
		the blockchain underlying the NFT[98]	professional skepticism and having an inquiring mind
	Internet of Things (IoT): Any device (with a built-in sensor) connected to the internet, creating a network of connected devices that collects and shares data about the people and/or environment around it	• Helps to collect and generate data that was previously not available or easily accessible, improving visibility and allowing for improved data analytics, especially when coupled with AI[101] • Remote asset management and monitoring, such as location tracking, including autonomous driving applications • Improve asset utilization, such as through predictive maintenance of industrial equipment and increased operational efficiencies through IoT-based process automation • Common examples of usage in everyday life already include smart	• Privacy and related issues relating to data collected[102] (i.e., could be of sensitive nature such as health data, have varying legal implications across jurisdictions) and "new" risks such as inadvertent collection of data from such devices • Expands the "attack surface" to penetrate a secure network,[103] see discussion on *Focus on Data Governance* • Challenges in quality control and compatibility (i.e., huge numbers of IoT devices that have different standards of quality and security) as well as connectivity (i.e., bandwidth) impact the successful functionality of IoT[104]

98 NASDAQ "Non-Fungible Tokens: Looking Beyond the Hype" (March 2022): https://www.nasdaq.com/articles/non-fungible-tokens-nfts%3A-looking-beyond-the-hype

101 Kamalika Some, "AI and IoT – 5 use cases where it's gathering pace" (February 2021) T_HQ: https://techhq.com/2021/02/ai-and-iot-5-use-cases-where-its-gathering-pace/

102 See, for example, Fritz Allhoff & Adam Henschke, "The Internet of Things: Foundational ethical issues" (September 2018) *Internet of Things* 1-2:55-66, online: https://doi.org/10.1016/j.iot.2018.08.005

103 As an example of how IoT devices can be compromised en masse, see Minh Duong, "How I hacked ALL displays in my high school district to play Rick Astley" (October 2021) TNW: https://thenextweb.com/news/how-i-hacked-high-school-rick-astley-rickrolling-syndication

104 IoT Now "5 challenges still facing the Internet of Things" (June 2020): https://www.iot-now.com/2020/06/03/103228-5-challenges-still-facing-the-internet-of-things/

Maturity[96]	Technology	Opportunities	Impact/Risks
		home and wearable devices	
	Digital 5G: The 5th generation of mobile networking with dramatically faster (i.e., by an anticipated 8 to 16 times) upload and download speeds than 4G networks	• Predictive intelligence in smart industrial settings and smart cities, including ties to sustainability[105] • Enhanced mobile broadband and speeding up large data transfers • Accelerating the development and deployment of IoT applications, including edge computing[106]	• Increase in 5G mobile powered digital transactions means that companies will need a streamlined way to authenticate users. Digital authentications will need to be more versatile, more frequent and more frictionless than before[107]
	Immersive digital worlds ("metaverse"): Enabled by augmented reality ("AR", which augments real-world scenes with additional information overlays) and/or virtual reality ("VR", which creates a completely virtual environment)	• Professional education and evaluation through simulations • Specific to audit firms, the pandemic has seen an increase in using AR and drones for remote inventory counting. Nevertheless, uptake is still slow mainly driven by reluctance from regulators and jurisdictional legislation	• Data privacy, cybersecurity concerns, and lack of identity verifiability[108] • Questions over harassment and discrimination in virtual worlds and the lack of research on the physiological impacts on humans of prolonged immersion in VR/AR environments[109]

105 See, for example, World Economic Forum and PwC, The Impact of 5G: Creating New Value across Industries and Society (2020: https://www.pwc.com/gx/en/about-pwc/contribution-to-debate/wef-the-impact-of-fiveg-report.pdf

106 IBM, "5G Will Accelerate a New Wave of IoT Applications": https://newsroom.ibm.com/5G-accelerate-IOT

107 Forbes "The Future Is Here: How 5G Is Revolutionizing Digital Identity" (February 2022): https://www.forbes.com/sites/forbestechcouncil/2022/02/03/the-future-is-here-how-5g-is-revolutionizing-digital-identity/?sh=2235869d33f6

108 TechTarget (June 2022): https://www.techtarget.com/searchcio/feature/10-metaverse-dangers-CIOs-and-IT-leaders-should-address

109 See, for example, Ben Kenwright, "Virtual Reality: Ethical Challenges and Dangers" (January 2019) IEEE Technology and Society: https://technologyandsociety.org/virtual-reality-ethical-challenges-and-dangers/

Maturity[96]	Technology	Opportunities	Impact/Risks
		that might not allow virtual inventory taking	• Transactions, many speculative at this point, are conducted in the metaverse will also have tax and financial reporting implications that are evolving
	Edge Computing: Real-time processing of data at the source by combining use of IoT with cloud computing	• Distinguished from cloud computing, which aggregates data collection from sources before processing it in the cloud • Improving response times and decision-making, and saving bandwidth by bringing computation closer to the source of data (i.e., important when facing today's supply chain issues) • Allows continuous learning and optimization of the process as data is processed real-time	• See discussion on *Technology Landscape: Cloud Computing*
	Web 3.0: Envisioned as the third generation of the internet built on a decentralized distributed ledger (i.e., blockchain) and where users can create and own their own data. Web 2.0 is today's internet built mainly on Javascript and HTML5, which allows user	• No central authority controlling the collection, ownership, and flow of information • Facilitates blockchain technology and concepts, including digital identity, smart contracts, DeFi and decentralized applications	• The notion of a "creator" economy will mean a rise in NFTs that serve as products or services which can be bought and sold on the blockchain underlying Web 3.0. Presents questions over data security; data ownership; digital identity; and the identification and mitigation of fraudulent

Maturity[96]	Technology	Opportunities	Impact/Risks
	interaction but where relatively few companies own user data, i.e., large technology companies[110]	(dApps)[111]. See section above on *Technology Landscape: Blockchain – Cryptocurrencies, Tokens and Decentralized Finance*	transactions, programming bugs and errors, etc. • See also discussion on *Technology Landscape: Blockchain – Cryptocurrencies, Tokens and Decentralized Finance*
	Quantum computing: Emerging technology that harnesses the laws of quantum mechanics to solve problems "too complex" for today's computers[112]	• Where today's supercomputers use a "two-dimensional" approach to solve statistical problems, quantum computing is anticipated to allow a new multi-dimensional approach to solving statistical problems, meaning that its computing power has increased significantly and can take into account an exponential number of multiple variables and uncertainties as compared to today's computers • Will innovate different method/approach of encryption in face of	• Impact on cybersecurity due to the increased computing power that will effectively render all of today's public-key encryption systems "useless". Accordingly, there will be a need to upgrade the technical security for every organization and entity[113]

[110] Wall Street Journal "Why Some See Web 3.0 as the Future of the Internet" (February 2022): https://www.youtube.com/watch?v=OEJGQD1OuKA

[111] Forbes "The Metaverse and Web3 Creating Value in the Future Digital Economy" (June 2022): https://www.forbes.com/sites/markminevich/2022/06/17/the-metaverse-and-web3-creating-value-in-the-future-digital-economy/

[112] IBM Quantum Computing "What is Quantum Computing?": https://www.ibm.com/topics/quantum-computing

[113] See, for example, US National Institute of Standards and Technology (US NIST), "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms" (July 2022): https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms; Patrick H O'Neill, "The US is worried that hackers are stealing data today so quantum computers can crack it in a decade" (November 2021) MIT Technology Review: https://www.technologyreview.com/2021/11/03/1039171/hackers-quantum-computers-us-homeland-security-cryptography/

Maturity[96]	Technology	Opportunities	Impact/Risks
		such massive computing power	
	Homomorphic encryption, part of a wider group of technologies called Privacy Enhancing Technologies (PETs): Allows data to be securely and privately used throughout its lifecycle without the need to decrypt it, meaning that different parties can be given access to work directly on the encrypted data without ever seeing the raw data[114]	• Allows businesses to comply with various jurisdictional data protection laws • Enables data testing by third parties[115] as PETs facilitate privacy protection while data sharing • Protects against privacy breaches that could potentially severely harm business reputation	• Computation overhead needs to be significantly decreased as it is still very slow, so not yet practical to use for many applications[116] • Additionally, integration challenges between data collection points, i.e., IoT (typically designed to consume low energy and storage), and PETs (running PETs typically requires greater computational power) • Trade-off between utility and privacy, presenting questions over data authenticity and integrity and reducing transparency in data, for example, impacting the assessment of data used to train AI models
	Cognitive AI: AI with cognitive abilities more similar to a human, including the	• Ability to mimic human behavior and respond to complex problems. See section above on	• Cognitive AI will impact decision-making and whether such decisions made by AI have

[114] See, for example, US NIST Cybersecurity Insights: Brandao LT & Peralta R, "Privacy-Enhancing Cryptography to Complement Differential Privacy" (November 2021): https://www.nist.gov/blogs/cybersecurity-insights/privacy-enhancing-cryptography-complement-differential-privacy

[115] Including use of client data by audit firms, see for example, *[placeholder for IAASB upcoming market scan on Homomorphic Encryption]*

[116] Forbes "What is Homomorphic Encryption? And Why Is It So Transformative?" (November 2019): https://www.forbes.com/sites/bernardmarr/2019/11/15/what-is-homomorphic-encryption-and-why-is-it-so-transformative/?sh=51bbc1ce7e93

Maturity[96]	Technology	Opportunities	Impact/Risks
	ability to make decisions in unforeseen environments	*Technology Landscape: AI*	human oversight, are understandable and explainable. See discussion on *Technology Landscape: AI*

Focus on Data Governance

90. Data governance is foundational to building and maintaining organizational value at both strategic and operational levels. It has become critical in today's data- and information-driven world, where technology and related decisions rely on quality data. Quality data has three characteristics: accuracy, completeness, and reliability.

91. Most organizations are flooded with data. Almost every action anyone takes leaves a digital trail. On top of this, the amount of machine-generated data is also growing rapidly. Data is generated and shared when "smart" home IoT devices communicate with each other or with their home servers. Industrial machinery in plants and factories around the world are increasingly equipped with IoT sensors that gather and transmit data.

92. Data itself is increasingly seen as a commodity and a source of strategic advantage, despite its not (yet) being recognized as an "asset" on the traditional balance sheet. However, the mere possession of abundant amounts of data is not enough. What is foundational is the ability to refine, process, and evaluate data and capture meaning from unstructured data that can tell a story to provide both strategic and operational value to an organization. In this regard, the level of activity (and type of value provided) in the data and analytics space over the last two years has generally evolved around four categories: [117]

- Descriptive, focused on what has happened.
- Diagnostic, focused on why it has happened.
- Predictive, used to forecast what could happen.
- Prescriptive, analyzed to help determine what should be done.

93. As outlined in the discussions on *RPA* and *AI technology trends, opportunities and impacts/risks*, organizations are also increasingly automating traditional manual, human-led processes, as well as utilizing AI for such data manipulation.

94. Successful automation is driven in part by consistent data, but a major challenge encountered by stakeholders is that typically there are legacy systems in organizations that are set up differently from

[117] See, for example:

- New Era of Data Science in Today's World (November 2020): https://data-science-blog.com/blog/2020/11/04/new-era-of-data-science-in-todays-world/
- Michigan State University "4 Types of Data Analytics and How to Apply Them" (October 2019): https://www.michiganstateuniversityonline.com/resources/business-analytics/types-of-data-analytics-and-how-to-apply-them/

each other. This increases the risk of error as the data are often both unstructured and not standardized.

95. In this regard, stakeholders reported that they expect PAIBs to be more involved in broader data governance matters to ensure quality data prior to relying on its use, whether for decision-making or as an input to automation. This is because PAIBs are well-positioned vis-à-vis their professional work for the organizations they support (i.e., internal controls and processes) and their involvement at every stage of the data governance cycle (i.e., from data generation or collection through to its use, transfer, storage, residency, dissemination, and lawful destruction). It is also because it is part of a PA's professional duty as data flows into the preparation and presentation of financial statements.

96. Accordingly, PAs are seen by some stakeholders as being accountable for the quality of such data. For example, some stakeholders indicated that it is critical for PAs to ensure that the data being used is accurate, complete, and reliable, regardless of whether the technology processing and storing such data was developed internally or sourced externally (i.e., hosted by an external cloud service provider or processed by externally developed bots).

97. In addition to data quality issues, the use of data raises potential ethics challenges.[118] For AI to produce the most valuable and accurate insights, training models need "real" data. However, stakeholders have questioned whether the use of actual data for this purpose engages the Code's fundamental principles of integrity and confidentiality. For example, even if a firm or a company obtains the consent of a client or customer to use data collected while performing a professional activity for the purpose of training an AI system under development, is this sufficient to meet the requirements of the Code's fundamental principle of confidentiality? Does this answer change if the data is anonymized first? Would this be considered similar to a request by third parties to use de-identified (i.e., anonymized) client information for purposes of publishing benchmarking data or studies?[119]

98. To meet the expectations for data quality and use, stakeholders noted that it is important to have a data governance and information stewardship framework in place that ensures, among other outcomes, the accuracy, objectivity, consistency, and completeness of data for use in decision-making and/or sharing with a third-party. When designing such frameworks, for example, as part of considering the appropriateness and effectiveness of internal controls over financial reporting, stakeholders highlighted that PAs should consider the appropriateness of governance around:

    - Controls over data integrity, that is, the source of data and whether it has been modified subsequent to its creation, collection, or acquisition.
    - Whether the data is representative for the purpose and population it is being used to serve or model.

---

[118] As an example of a tool to help identify and manage ethics issues related to data governance, see the Open Data Institute's "Data Ethics Canvas", available online at https://theodi.org/article/the-data-ethics-canvas-2021/#1563365825519-a247d445-ab2d

[119] In this regard, a stakeholder noted that the AICPA Code paragraph 1.700.060 "Disclosure of Client Information to Third Parties" states that threats to compliance with paragraph 1.700.001 "Confidential Client Information Rule" may exist in cases which may result in the client's information being disclosed to others without the client being specifically identified. Such rule states that PAPPs shall not disclose any confidential client information without the specific consent of the client.

- Understanding the nature of the data being created, collected, or acquired – including the related implications for compliance with professional obligations and jurisdictional legislation or regulation with respect to confidentiality and privacy.[120] This includes understanding, for example, where the data will reside and how it will eventually be disposed of.
- Distinguishing between commercial and personal or individual information that could be potentially sensitive and have differing legal implications, for example, innovative intellectual property or medical information.
- Emerging issues such as the "ownership" of "new" data created from big data mining and applying AI to existing data sets.
- Reasonableness of risk identification procedures pertaining to the data governance cycle, controls to address such risks, documentation requirements, and ongoing management.
- Collateral risk assessments of breaches in confidentiality and privacy that such breaches, or cyber-attacks or ransomware, demand, as well as related contingency plans.

99. Additionally, stakeholders indicated that the ease with which mis- and disinformation is spread is a pervasive issue in society that should be considered as part of data governance and information stewardship.[121] In this regard, the Working Group notes that PAs can think of meeting professional obligations for objectivity, integrity, professional competence and due care, and their public interest responsibilities in the face of bias and mis- and disinformation in terms of four layers: [122]
    - Layer 1: Taking care to produce information that is accurate and objective.
    - Layer 2: Ensuring that information the PA relies on is reliable.
    - Layer 3: Not passing on mis- and disinformation.
    - Layer 4: Proactively countering bias and mis- and disinformation.
100. The main challenges that stakeholders reported facing with respect to data governance arise from the volume and quality of data, the number of data privacy policies to be complied with across jurisdictions (e.g., the European Union's General Data Protection Regulation (EU GDPR)), the multitude of communication platforms (i.e. shadow IT platforms[123] such as Slack) and what is being communicated over such platforms (i.e. confidential agreements shared through such platforms due

---

120 Concerns around data collection and use pertain to both internal and external stakeholders. For example, a 2019 Accenture report notes that "While more than six in 10 C-level executives (62 percent) said that their organizations are using new technologies to collect data on their people and their work to gain more actionable insights — from the quality of work and the way people collaborate to their safety and well-being — fewer than one-third (30 percent) are very confident that they are using the data responsibly." See Accenture's press release that summarizes the results at https://newsroom.accenture.com/news/more-responsible-use-of-workforce-data-required-to-strengthen-employee-trust-and-unlock-growth-according-to-accenture-report.htm

121 A significant example of this issue, albeit within a political advocacy context, is described in New York State Office of the Attorney General, "Fake Comments: How US Companies & Partisans Hack Democracy to Undermine Your Voice" (2021): https://ag.ny.gov/sites/default/files/oag-fakecommentsreport.pdf

122 CPA Canada, ICAS, IFAC & IESBA, *Identifying and Mitigating Bias and Mis- and Disinformation* (February 2022): https://www.cpacanada.ca/en/foresight-initiative/trust-and-ethics/%20identifying-mitigating-bias-mis-disinformation

123 Shadow IT and IoT – the use of unauthorized applications, clouds, and internet of things devices and networks outside an organization's formal IT enterprise environment

to a lack of related formal guidelines), and cybersecurity risks associated with data transmission and storage.[124]

Cybersecurity

101. Cyberattacks have become an organizational reality and stakeholders observe three frequent targets: (a) financial systems, (b) intellectual property, and (c) intelligence, for example, information and analysis about an organization, individuals, or a jurisdiction.

102. In most cases, security gaps are created by human behavior, for example, an individual unknowingly clicking a malicious weblink or installing an insecure device.[125] Digitalization and remote working are affecting all organizations, increasing the available cyberattack surface area, namely the available points that are exposed for attackers to target.[126] For example, the connection of generally less secure IoT devices within corporate digital ecosystems creates potential gaps in enterprise security.[127] Similarly, increased digitization leads to greater potential for social engineering where inadequately trained employees also have access to increasingly complicated, and interconnected, systems.

103. Stakeholders highlighted that PAs and others in the organization need to work together to ensure data protection, confidentiality and, where relevant, privacy of organizational data. Despite an exponential increase in cybersecurity risk, stakeholders observed frequent challenges within individual organizations to obtain sufficient investment budget and resources to address such risk, often finding that enhanced mitigations are implemented only after a breach or other failure.[128]

104. Stakeholders indicated that it is crucial for organizations to recognize that, often, customer data are the most valuable assets that organizations can hold, and that although investment in cybersecurity to protect such assets might be costly, the aftermath of a cyberbreach is typically an order of magnitude more costly and more challenging to address. It was observed that the biggest advocates of cybersecurity tend to be TCWG, such as audit committees and internal audit groups. Risk committees, where they exist, also help to drive the cybersecurity agenda, but might have challenges with quantifying the likelihood of cyberthreats.

---

[124] US Public Company Accounting Oversight Board (PCAOB) "2021 Conversations with Audit Committee Chairs" (March 2022): https://pcaobus.org/documents/2021-conversations-with-audit-committee-chairs-spotlight.pdf

[125] See, for example, Verizon, *2022 Data Breach Investigations Report* (2022): https://www.verizon.com/business/resources/reports/dbir/ that found 86% of breaches involved a human element and Niloo Razi & Matt Polak, "The Twitter Hack Shows a Major Cybersecurity Vulnerability: Employees" (July 21, 2020) Slate: https://slate.com/technology/2020/07/twitter-hack-human-weakness.html

[126] See, for example, Rico Brandenburg & Paul Mee, "Cybersecurity for a Remote Workforce" (July 23, 2020) MIT Sloan Management Review: https://sloanreview.mit.edu/article/cybersecurity-for-a-remote-workforce/; Catherine Stupp, "As Remote Work Continues, Companies Fret Over How to Monitor Employees' Data Handling" (August 21, 2020) Wall Street Journal: https://www.wsj.com/articles/as-remote-work-continues-companies-fret-over-how-to-monitor-employees-data-handling-11598002202; Liam Tung, "FBI warning: Crooks are using deepfakes to apply for remote tech jobs" (June 2022) zdnet: https://www.zdnet.com/article/fbi-warning-crooks-are-are-using-deepfakes-to-apply-for-remote-tech-jobs/

[127] See, for example, Lily H Newman, "100 Million More IoT Devices Are Exposed–And They Won't Be the Last" (April 13, 2021) Wired: https://www.wired.com/story/namewreck-iot-vulnerabilities-tcpip-millions-devices/

[128] For thoughts on where executives, such as CFOs, should be evaluating risks and the budget needed to cover them, see Vincent Ryan, "Budgeting for Cybersecurity Requires a New Approach" (September 7, 2021) CFO: https://www.cfo.com/budgeting-planning/2021/09/budgeting-for-cybersecurity-requires-a-new-approach/

105. Suggestions from stakeholders and through other research about how to be aware, vigilant, and prepared include ensuring a sufficient investment budget and dedicated resources so that:

- An incident responder, who already understands the business, is retained and accessible before an issue happens.
- A cyber-response plan is ready for all types of foreseeable cyberattack possibilities (i.e., the plan should consider the speed of an entity's response to an attack and under what circumstances the entity will, for example, pay ransomware, as well as the related policies and procedures it will follow).[129]
- There is frequent and proactive updating of technology and that a layered approach[130] to cybersecurity is applied.
- There are regular cybersecurity assessments or scans conducted to test vulnerability.[131] For example, continuous intrusion detection and prevention, regularly inventorying IT assets connected to the organization (including how many digital assets there are, who owns them, and who is accountable for them), and periodic penetration testing to understand what is exposed.
- There is ongoing employee education, such as the incentivization of proactive security behavior ("cyber-vigilance") and establishing a security culture across the organization that includes sufficient access protection and appropriate controls over data and private keys or passwords.[132]

106. With respect to cybersecurity issues and the broader area of data governance, stakeholders emphasized that there are significant expectations and opportunities for PAs to play an active role in overseeing the impacts on their organizations and clients, as part of the PAs' ethical obligation to be competent, exercise due care, and act in the public interest.

107. The Working Group notes that the technology landscape as outlined in this subsection is fast evolving and that PAs should maintain an awareness of the developments in technology,[133] and the related

---

[129] For commentary on the ethical and legal implications of paying a ransom to cyberattackers, see Vinita Srivastava, "Colonial Pipeline forked over $4.4M to end cyberattack–but is paying a ransom ever the ethical thing to do?" (May 26, 2021) The Conversation: https://theconversation.com/colonial-pipeline-forked-over-4-4m-to-end-cyberattack-but-is-paying-a-ransom-ever-the-ethical-thing-to-do-161383; Elizabeth Lopatto, "Ransomware funds more ransomware, so how do we stop it?" (June 24, 2021) Verge: https://www.theverge.com/2021/6/24/22545675/ransomware-cryptocurrency-regulation-hacks; US Department of the Treasury "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments" (September 2021) online: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf

[130] Layered security is a security approach that deploys multiple layers of security control that back one another up in the event one is breached or fails, for example, employing effective network, system, application, human, and physical elements as part of a complete defense strategy. This is particularly important when protecting the most critical data and information within an organization's technology environment.

[131] Additional ideas are contained, for example, in the US Cybersecurity & Infrastructure Security Agency's *CSET Ransomware Readiness Assessment*: https://www.cisa.gov/uscert/ncas/current-activity/2021/06/30/cisas-cset-tool-sets-sights-ransomware-threat

[132] This might include, for example, "common sense" security procedures for individuals to follow, such as multi-factor authentication (MFA) when accessing data or systems.

[133] Paragraph 113.1 A2 of the Code

opportunities and impact/risks, so that they can better identify threats to compliance with the fundamental principles of the Code, and accordingly, evaluate and address such threats.

C. Potential Ethics Impact on the Behavior of PAs

108. 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.[134]

Competence and Due Care

Need for Competence in the Digital Age

109. The business world today is dynamic, complex,[135] and broad, with many grey areas. The vast amount of data that is available far exceeds the human mind's ability to process and understand it.[136] There continue to be significant changes and developments in technological innovation, as well as in standards and regulations. Against this backdrop, the Working Group notes that the competence of PAs needs to adapt to meet the profession's responsibility to act in the public interest and to rise to opportunities. This competence gap is not limited to PAs, of course, but rather is also relevant for all actors in the business and finance ecosystem, including regulators.

110. Stakeholders stressed that PAs have a great deal to keep up with and there is a growing need to use technology to manage complexity and leverage opportunities arising from emerging technology and the availability of data. In particular, it is also noted that SMPs (who make up a large proportion of PAPPs), and particularly sole practitioners, have significant time and resource constraints, which makes "keeping up" more challenging and potentially creates a bigger competency gap risk. However, PAs might still be drawn to the alure of leveraging the opportunities and efficiencies of technology despite lacking the requisite competence.

111. Stakeholders further reported that investment in, and accessibility of, online training has exponentially exploded across organizations. However, they also indicated that training junior staff (i.e., candidates to the accountancy profession) to apply professional judgment is becoming more challenging as automation and AI take over more tasks and processes that junior staff were once completing as part of their qualifying period of practical experience. This potentially creates a gap in understanding the

---

134 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.

135 CPA Canada, ICAS, IFAC & IESBA, *Complexity and the professional accountant: Practical guidance for ethical decision-making* (June 2021): https://www.cpacanada.ca/en/foresight-initiative/trust-and-ethics/complexity-guidance-ethical-decision-making.

136 Tim Maughan, "The Modern World Has Finally Become Too Complex for Any of Us to Understand" (November 29, 2020), online OneZero: https://onezero.medium.com/the-modern-world-has-finally-become-too-complex-for-any-of-us-to-understand-1a0b46fbc292

"basics" and being ready to effectively oversee the work of autonomous and intelligent agents. It was suggested that the application of VR and other immersive platforms might assist in mitigating these sorts of issues by providing or supplementing such experience through simulations.

112. On a related note, concerns were also raised by stakeholders that junior staff might be considered more technology-literate than they really are, resulting in an over-reliance on such staff when using certain technologies. Despite junior staff growing up in an environment where "technology is everywhere," they often do not have specific experience with some of the key transformational technologies being developed and implemented by organizations (e.g., machine learning, blockchain, and data analytics tools).

113. Specific to PAs, stakeholders viewed traditional accountancy skills as core "table stakes," whereas more breadth in both technology upskilling and enhancing professional skills is seen as being a priority.[137] Stakeholders also noted that it is important for PAs to recognize that developing, implementing or using technology is not just an IT department issue – PAs need to have sufficient competence to enhance their opportunity to be part of the decision-making process and address potential issues arising from technology. For example, managing financial and related systems, business processes, policies, and controls is traditionally the domain of PAs (and not IT professionals). PAs, however, need to have sufficient competence in emerging and transformative technology and data literacy to adapt these traditional skills to the new context. Therefore, the application of professional skills as necessary for managing multidisciplinary teams that consist of IT and other professionals, and cross training between IT and accounting, is increasingly critical and of significant benefit and value for organizations and firms.

114. There is general acknowledgement from stakeholders that whereas PAs do not need to be the "experts" in technology, they nevertheless need sufficient competence in the area. Naturally, this raises questions around what is considered "sufficient" competence and how this changes depending on the PA's position and role within the organization. This is particularly important as typically senior-level PAIBs[138] are responsible for signing off on IT controls over financial systems. These PAs must therefore understand the risks and processes, and what should be done to mitigate those risks. In addition, a few stakeholders wondered whether there should be guidelines on sufficient professional competence for PAPPs in relation to technologies implemented by their clients, as this would better help firms determine whether to accept or decline professional engagements on this basis and where to allocate training resources.

115. Stakeholders generally describe "sufficient" competence as knowing enough about how the technology works in order to:

    (a) *Ask* IT professionals appropriate questions and *understand* their responses in the context of the system or tools being assessed;

    (b) Have *confidence* in what is happening with the system or tool; and

---

137 See, for example, CPA Canada, ICAS, IFAC & IESBA, *Mindset and enabling skills of professional accountants – a competence paradigm shift* (April 2022): https://www.cpacanada.ca/en/foresight-initiative/trust-and-ethics/mindsets-professional-accountants

138 In some instances, stakeholders reported observing that organizations are folding the role of Chief Information Officer/Chief Technology Officer (CIO/CTO) with that of the Chief Financial Officer (CFO) role given that enterprise resource planning systems used for accounting and finance are "overseen" by internal control processes and might be the largest IT package that a company maintains.

(c) Be able to *justify* the use and outputs of the tool.

In this regard, the subsection below on *Technology Upskilling Needed* describes in detail what stakeholders believe this entails in a practical sense. However, stakeholders acknowledged that it is impractical to define specific thresholds for "sufficient" competence for technology overall given its broad and dynamic nature, varied applicability, the range of PA roles interacting with different technologies, and the need for contextual professional judgment. It was also observed that because of the complex business environment, focus has shifted from achieving a certain depth of knowledge at a point in time, to continuously keeping up with what is going on in a broader context – what some stakeholders referred to as "life-long learning."

116. As a result, initial and continuing professional development (IPD and CPD) must continue to evolve to ensure, among other matters, that the necessary technologies (i.e., basic computing, data analytics, AI, blockchain, and other related concepts/skills, such as the difference between structured and unstructured data) are integrated into training and professional development programs. Already, significant changes are being made to numerous accounting curricula at universities and through PAOs and in CPD programs.[139]

Technology Upskilling Needed

117. The Working Group observes that deeper technology-related skills will enable PAs to leverage the tremendous opportunities and benefits offered by technology, as well as to enhance the opportunity for PAs to be at the technology decision-making table and help serve as ethical stewards by asking the right questions, explaining the potential ethics implications of decisions, and assisting in choosing appropriate technology solutions. However, as also noted in the discussions on *Ethical Leadership* and *Need for Competence in the Digital Age*, stakeholders repeatedly emphasized the broad perception that there might not be enough trust in PAs to be at the table because PAs are not seen to have mastered the "language" and fundamentals of innovative and disruptive technologies. For example, stakeholders observed that:

- PAs often lack relevant practical experience and knowledge about AI, blockchain (including cryptocurrencies[140]), and data governance to know what type of questions to ask, how to identify specific risks and errors and the related mitigation remedy, and how to assess the reliability of these transformational technologies. There is a further concern around the

---

139 For example, CA ANZ's qualification program now includes some technology and ethics-related modules, including Ethics and Business, Risk and Technology, Data Analytics and Insights: https://www.charteredaccountantsanz.com/become-a-member/apply-for-the-ca-program/ca-program-overview; CPA Evolution Model Curriculum developed by NASBA and AICPA to assist faculty who want to prepare their students for the CPA profession, and which has considered the need for newly licensed CPAs to have deeper skill sets, more competencies and greater knowledge of emerging technologies: https://nasba.org/wp-content/uploads/2021/06/Model-curriculum_web_6.11.21.pdf; CPA Canada's Competency Map 2.0, which significantly reimagines the skills and competencies required by future accountants in the context of emerging opportunities, the influence of automation, and increased interconnectedness: https://www.cpacanada.ca/en/become-a-cpa/why-become-a-cpa/the-cpa-certification-program/the-cpa-competency-map/competency-map-2-0

140 See, for example, Sonia Sharma, "Advisers must deepen understanding of cryptoassets as client demand increases, industry figures say" (August 2022) AccountancyAge: https://www.accountancyage.com/2022/08/10/advisers-must-deepen-understanding-of-cryptoassets-as-client-demand-increases-industry-figures-say/ and Lindsey Choo, "You might be evading crypto taxes and not even know it" (April 2022) Protocol: https://www.protocol.com/fintech/crypto-taxes-staking-mining-airdrops

consequences of PAs being the end users of such technology and relying on the outputs relative to a lack of sufficient competence.

- PAs tend to have insufficient knowledge about cybersecurity, which is key to safeguarding the data under their charge and upon which they rely to support decision-making. In fact, it was suggested that most individuals, including PAs, do not know how to protect themselves and their own devices from cyberattacks.

118. Stakeholders outlined five key areas of technology upskilling they believe are necessary as digital transformation changes the profession. This upskilling will permit PAs to not only uphold their professional obligations of professional competence and due care, but also earn their place at the decision-making table to advise strategically and knowledgably on the risks and benefits of technology development, implementation, and use in organizations and firms. Unsurprisingly, due to the volume of, and reliance on, data, the most cited area of upskilling is data-related skills and concepts. For example, PAs need to be able to determine that data used for data analytics, RPA, or AI is high quality and fit-for-purpose (see discussion on *Focus on Data Governance*).

119. Stakeholders also provided specific examples of skills they believe are important in each of these five key areas. These examples largely relate again to the key upskilling area of data-related skills and concepts:

Upskilling Area	**Specific Examples Highlighted by Stakeholders as Important**
Data-related skills and concepts	• How to classify data (critical vs non-critical) • What is confidential and "how" confidential • Determining the quality of data • Consequences (intended and unintended) of data collection, use, storage and destruction across the stages in the data value chain • Data analytics (incl. for forecasting and strategy) • Data visualization • Auditing data sets • Ensuring data completeness
Technology Capability	• Effectiveness of control environment • Identification of risks • How technology is used to manipulate results (fraud)
Cybersecurity	• Cyber-attack techniques • Cyber-regulations • Maintaining privacy, incl. potential liability if privacy regulations are breached

Upskilling Area	Specific Examples Highlighted by Stakeholders as Important
Foundational IT	• Source code understanding • Basic level of programming
AI	• Assessment of intelligent agents

120. Stakeholders noted that PAs should be encouraged to recognize the relevance of technology to the performance of their professional activities and develop the appropriate competence to use technology. In addition, a few stakeholders suggested that more technology-savvy PAs could also perform third-party certifications to ensure that technology is operating as intended. This is seen as a good fit because PAs can apply their traditional skillset of identifying the risks and controls pertaining to business processes to a technology implementation context, coupled with the application of ethics.

121. Finally, stakeholders observed that firms and organizations have moved to hiring individuals into their accounting or audit teams with wider or different, but complementary, skillsets than a traditional accounting and auditing background. Commonly sought-after skills include transformational technologies, data governance and analytics, and cybersecurity.[141] This largely matches the areas of proposed upskilling, further underscoring the demand for competence in these areas and the perceived gap in the existing PA space. Note that although IPD can be changed relatively quickly in many jurisdictions and institutions (perhaps 12-24 months), upskilling existing PAs through CPD is normally much more challenging and time consuming (even if introducing the courses themselves might be faster than through IPD).

Application of Core Accounting-related Skills Integrated with Professional Skills, Values, Ethics, and Attitudes

122. Stakeholders view that many of a PA's current core accounting skills are particularly valuable and transferable when applied appropriately in the context of emerging and transformative technology. For example, PAs have significant business intelligence and regularly establish business cases, optimize business processes, and establish control frameworks. These are important aspects to apply in activities such as considering a potential investment in new technology, identifying relevant risks, and implementing and documenting effective processes and controls. In particular, stakeholders commented that PAs, such as CFOs and their finance and accounting, planning, and analysis teams, traditionally play a central role in times of business or financial crisis to help organizations navigate and mitigate shock and disruption to the business eco-system. PAs are

[141] Note, for example, that some post-secondary institutions are seeking to fill such perceived skill gaps through the development of new graduate-level programs, such as York University's Master of Financial Accountability. This program promotes the acquisition of "strong critical knowledge and practical skills from across the areas of accountability, assurance, climate change, compensation, cyber security, ethics, governance, law and risk management" and does not lead to professional accounting credential – see https://mfac.gradstudies.yorku.ca/about/. These are important matters to consider as PAOs evolve their competency frameworks for IPD and CPD.

considered well positioned to deal with such complexities due to their professional training and broad problem-solving skillsets.[142]

123. Complex circumstances[143] are exacerbated in today's digital age by the ongoing rapid confluence of advancing technologies; increasing data creation, availability, and its interconnectedness; and emerging laws, regulations, and public expectations around novel approaches to transactions, finance, business models, tax planning, and sustainability. PAs need to recognize the significant digital transformation that is happening and understand its broader implications to compliance with the Code's fundamental principles and approaches to the professional activities they perform. PAs also need to complement their existing skillsets and behavior with the relevant upskilling and competence required for the profession to remain relevant.

124. Specifically, stakeholders emphasized that having the right mindset and applying professional skills, values, ethics, and attitudes[144] are essential for PAs to continue to serve as trusted advisors. This, in particular, continues to differentiate humans and machines and echoes the theme documented as part of the Working Group's thought leadership work.[145] In addition, the Working Group notes that although some PAs shy away from embracing the use of technology, it is critical that PAs leverage technology so that it complements, supplements, and elevates human judgment, rather than trying to replace it.

125. For example, some stakeholders observed that companies sometimes make decisions purely based on data, neglecting the value of human input in terms of professional judgment considering the facts and circumstances at hand. Significant negative consequences can be expected where humans are not kept in the loop (i.e., human involvement) of automated processes or decision-making, for example, to perform reasonableness checks and to bring an element of alertness for issues with data integrity and bias.[146]

126. The important non-technical skills that stakeholders highlighted as differentiators between PAs and autonomous and intelligent systems include:

    - Professional skills: PAs should be encouraged to think broader than their functional role, adopt enterprise-wide thinking, and be more well-rounded. Applying professional skills helps to facilitate effective oversight of teams (including the use of technology), strategy creation, and decision-making, as more routine and mechanical tasks are being automated. Professional skills include:

---

142 For examples of how AI and big data analysis can augment the work of PAs in addressing complex issues, such as supply chain disruptions in times of crisis, see Will D Heaven, "How AI digital twins help weather the world's supply chain nightmare" (October 26, 2021) MIT Technology Review: https://www.technologyreview.com/2021/10/26/1038643/ai-reinforcement-learning-digital-twins-can-solve-supply-chain-shortages-and-save-christmas/

143 *Supra* note 133

144 See for example, International Education Standard 3 and 4, *Professional Skills*: https://education.ifac.org/part/ies-3, and *Professional Values, Ethics and Attitudes*: https://education.ifac.org/part/ies-4

145 CPA Canada, ICAS, IFAC & IESBA, *Mindset and enabling skills of professional accountants – A competence paradigm shift* (April 2022): https://www.ifac.org/knowledge-gateway/building-trust-ethics/publications/mindset-and-enabling-skills-professional-accountants-paper-4

146 There are also potential risks of over-reliance and bias created by introducing human oversight that should be considered when designing systems. See, for example, Ben Green & Amba Kak, "The False Comfort of Human Oversight as an Antidote to AI Harm" (June 15, 2021) Slate: https://slate.com/technology/2021/06/human-oversight-artificial-intelligence-laws.html

- Communication skills to build strong and collaborative teams.
- Entrepreneurial skills that support innovation, creativity, disruption, and thinking outside of the box.
- Emotional intelligence, such as negotiation, influencing, persuading, and conflict management.

All PAs are expected to have technical skills. As mentioned in the discussion on *Need for Competence in the Digital Age*, such skills are now being deemed as table stakes. However, professional skills are becoming regarded as important, if not more so, in some situations.[147]

- Professional judgment and an inquiring mind: Part of a PA's value proposition is their training and experience to exercise professional judgment and be inquisitive, i.e., have an inquiring mind. Whereas there is a risk that machines will overtake human decision-making in the future, PAs are still well positioned to exercise their core skills of professional or business judgment. At the same time, PAs can resist undue influence from, or overreliance on, technology. They can also remain aware of and mitigate the effect of bias.

  Stakeholders noted that these core judgment skills are particularly critical when procuring and using or relying on AI. For example, PAs in charge of such functions can behave ethically by exercising professional judgment and having an inquiring mind to ask questions to ensure that the AI under consideration is fit for purpose, that the data inputs are fair and "free" from bias (i.e., that at least the bias is acknowledged and accounted for when evaluating the outputs), and that the information or output generated by the AI system makes sense.

- Mindset and attitude: The complexity of today's digital world – where, among other factors, technology, laws and regulations, and socially responsible and acceptable good practices and public expectations are constantly evolving – means that having the right mindset and attitude is important to stay current. Stakeholders described the right mindset in this context as proactively seeking out new learning opportunities, which some referred to as a "growth mindset," to promote life-long learning. In addition, because the world is not typically a binary delineation between "right" and "wrong," but rather is increasingly about managing uncertainty and complexity, having the right attitude, such as being accountable for one's own actions as part of a larger team, is key. This is seen as being well aligned with a PA's acceptance of their professional responsibility to act in the public interest.

Need for Diligence/Due Care

127. As documented in the Working Group's thought leadership work,[148] diligence and due care are needed to enable competent decision-making and service to clients and employers around transformational technology. Such transformational technology often present circumstances with increased complexity, dynamism and automation bias, increasingly sophisticated mis- and disinformation, and security threats (internal and external). However, it is important to recognize

---

147 See, for example, Ryan Chabus, "Top Soft Skills for Accounting Professionals" (June 7, 2021), online AICPA Journal of Accountancy: https://www.journalofaccountancy.com/newsletters/2021/jun/top-soft-skills-accounting-professionals.html, which reports that in a recent survey by the Society for Human Resource Management, 97% of employers stated that soft skills were either as important or more important than hard skills.

148 *Supra* note 133

practical limitations, including being intimidated or overwhelmed by technology and the pace of technological and regulatory change. PAs must also recognize that one cannot have access to all relevant information in real-time when decisions need to be made, and that the information available might well be the best that exists at that time. The consequences of decisions should, therefore, be monitored, and actions adapted, as additional data or information becomes available. This is the essence of managing complex circumstances.

128. In particular, stakeholders stressed that higher levels of due care are needed around ensuring that:

- Technology used is fit-for-purpose. It is observed that it will become incumbent on technology providers to prove that the technology is doing what it is supposed to; make AI systems interpretable so that PAs and others are able to understand the system's decision-making process and be able to assess the reasonableness of its outputs; and ensure appropriate data governance practices are applied to enhance trust. These are seen as key areas where PAs should challenge technology providers.[149]
- Data created, collected, or acquired and used is secure and handled appropriately. The stewardship and security of data are important. PAs must recognize the need for cyber-vigilance in light of threats to help ensure breaches do not occur with respect to the data flowing through their systems and processes. See discussion on *Focus on Data Governance*.

Objectivity

129. A PA is required to be objective,[150] which means to exercise professional or business judgment without being compromised by:

- Bias;
- Conflict of interest; or
- Undue influence of, or undue reliance on, individuals, organizations, technology or other factors.

In this regard, the Code prohibits a PA from undertaking a professional activity if a circumstance or relationship unduly influences the PA's professional judgment regarding that activity.

130. Stakeholder outreach indicated that whereas relying on technology brings about many significant opportunities for value creation, a delicate balance needs to be achieved to ensure there is no undue reliance on technology. Stakeholders highlighted several circumstances perceived as increasing the risk of threats to compliance with the principle of objectivity, including:

(a) Bias – Objective decision-making is hampered by bias in PAs. Stakeholders also remarked that bias can be manifest in numerous technology implementations, such as in the data used as inputs or in the programming of the technology. Accordingly, PAs using or relying on the

[149] For some ideas on what PAs might consider when choosing a technology to adopt, and what questions to ask of technology providers, see, for example, Deloitte Insights, "Beyond Good Intentions" (October 27, 2021): https://www2.deloitte.com/us/en/insights/industry/technology/ethical-dilemmas-in-technology.html and Patrick Hall & Ayoub Ouederni, "Seven Legal Questions for Data Scientists" (January 19, 2021), O'Reilly: https://www.oreilly.com/radar/seven-legal-questions-for-data-scientists/

[150] Paragraphs R112.1 and R112.2 of the Code

output of technology should be aware of the potential of such bias when assessing the reasonableness of relying on, or using, that output.

(b) Over-reliance – Reliance on technology tools and outputs is an important aspect of decision-making. However, objective decision-making is impeded by PAs becoming over-reliant on technology, especially where there is a lack of technical competence and/or where the technology lacks transparency and explainability.

(c) Transparency and Explainability – In order for technology to be relied upon, it needs to be understandable (i.e., the PA has the ability, or has access to a technology expert who can explain such technology to enable a PA, to understand, assess the reasonableness of, and explain the output of the technology, having regard to the purpose for which it is to be used). For example, this might include assessing the appropriateness of how data is processed, understanding the rationale for automated decisions, and being able to justify the reliance on, or use of, the outputs of the tool.

Bias

131. Bias is driven by human behavior and societal values that are impacted by, among other factors, one's education, experience, and cultural upbringing. As a consequence, bias is inherent in all datasets, technology programming, and laws and regulations.

132. Stakeholders stressed the importance of recognizing that there is inherent bias in data, which is particularly relevant to implementing and using AI systems. This includes data either used to train or test the system or as inputs for the system to process. Apart from data, AI systems also suffer from bias due to human programming. It is observed that there is increasing litigation on the basis of algorithm bias leading to unfair judgments, for example, for credit loans declined due to racial profiling or the inappropriate use of facial recognition.[151]

133. Furthermore, stakeholders noted that PAs should seek to understand how bias is identified, considered, and mitigated in the creation, capture, and analysis of data in systems, including how the "human element" impacts the AI training. Asking appropriate questions[152] and analyzing output to facilitate such understanding are key to mitigating the effect of bias. Stakeholders also emphasized that additional guidance related to such risk, and how it can be identified and mitigated, is needed.

134. The discussion in *Technology Landscape: Artificial Intelligence* outlines some actions for PAs to combat bias in AI systems. These actions are summarized as: (a) understanding the data going into the model, (b) understanding how the model operates, what the intended outputs are, and the potential unintended consequences of the model, (c) having the ability and competence to ask the effective questions, (d) ensuring a "human-in-loop" approach, and (e) promoting an ethics-based organizational culture.

---

[151] See, for example, Bloomberg Law, "Bias in Artificial Intelligence: Is Your Bot Bigoted?" (October 2020): https://news.bloomberglaw.com/tech-and-telecom-law/bias-in-artificial-intelligence-is-your-bot-bigoted; George Washington University, *AI Litigation Database*: https://blogs.gwu.edu/law-eti/ai-litigation-database/; and McCarthy Tétrault, "Could AI get you sued? Artificial intelligence and litigation risk" (April 2022): https://www.mccarthy.ca/en/insights/blogs/techlex/could-ai-get-you-sued-artificial-intelligence-and-litigation-risk.

[152] See, for example, Exploring the IESBA Code, A Focus on Technology – Artificial Intelligence (March 2022) *https://www.ifac.org/knowledge-gateway/supporting-international-standards/publications/exploring-iesba-code-focus-technology-artificial-intelligence*

Over-reliance

135. Stakeholders reported that since the beginning of the COVID-19 pandemic, daily decisions have become more challenging with the increase in remote meetings and reliance on technology.[153] For example, this reliance on technology can impact the PA's ethics obligations to act with due care, be objective, and maintain confidentiality (including respecting data privacy). In particular, stakeholders noted that:

- People are increasingly simply deciding that the machine is "correct" (i.e., displaying automation bias).[154]

  This calls into question how various accounting or auditing matters are decided – by the human or the machine. It also highlights the importance of assessing the effectiveness of the tool or system being used, and mitigating bias (i.e., ensuring that the algorithms do not make inappropriate judgments).

- Reliance on technology, for example, using an automatically generated report, reduces foundational training of less experienced team members and might deepen automation bias.

  Less experienced team members, who were never involved in creating the report and understanding its purpose, will have less ability to recognize or identify what might be unreasonable or incorrect, and likely will not be able explain the report's basis. See also the discussion on *Competence Need in the Digital Age*.

  It was also noted that if such automatic reports are generated regularly enough, even more experienced team members will stop noticing what might be incorrect or omitted.

- Organizations and firms are looking for technology that can easily and rapidly increase revenues and/or reduce costs and time to make decisions.

  Some smaller and middle market PAPPs, for example, are looking for technology to shorten their project timeframes, believing that it will immediately alleviate the impact of competitive fee pricing in the face of staff shortages and ever-tighter deadlines. Stakeholders noted, however, that such "silver bullet" technology is often not fully tested and not yet proven. This means that its use could raise data integrity and security issues, and create material impacts on workflows that might result in unintended consequences, such as audit failures and reputational damage. It is important to recognize that whereas a mistake by one staff member on a single client might have relatively few long-term implications, implementing untested or unproven technology risks an entire process that is poorly automated and might impact numerous clients before the defects are caught.

- Technology tools and systems developed by recognizable "brand names" are often immediately trusted. This is despite the documentation of the technology's source code or the detailed quality assessment processes underpinning its development generally not being made available by the technology developer. This is seen as a particular concern for small- and mid-sized organizations and firms in terms of sufficiently understanding the technology being used,

---

153 https://www.ethicsboard.org/focus-areas/covid-19-ethics-independence-considerations

154 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

given that they have less "bargaining power" than larger organizations to obtain such valuable (i.e., proprietary) information.

- When third-party tools are implemented by external consultants, organizations often lack the internal competence and resultant accountability to take responsibility for such tools and related outputs after the consultants complete the engagement.
- Analytical tools and digital assistants are becoming increasingly commonplace and improving with time and technological advancement.

  Some stakeholders, particularly technologists, wondered at what point it becomes possible to stop trying to learn about the underlying technology and simply place trust in the system. They observed the parallel of relying on a digital tool (or digital assistant, see discussion on *Technology Landscape: Robotic Process Automation*) to relying on a supervised human staff member.

  These stakeholders believed that the level of "trust" should be the same threshold used to assess reliance on the work of others in the Code. Some stakeholders also noted that this issue of "distrusting" technology is related to the ability to explain the decisions made by, or the outputs of, autonomous and intelligent systems and tools. They cautioned that this would be of increasing significance as developments in cognitive AI advance.

136. Finally, stakeholders noted that to mitigate automation bias and over-reliance on technology, PAs need to be aware of the various blind spots where errors could occur when digitalizing. For example, using unstructured data in AI to evaluate anomalies in contracts might result in potential optical character recognition (OCR) errors due to poor key words and structuring, as well as issues in machine learning algorithm processes such as natural language processing (NLP).[155]

Transparency and Explainability

137. Many current AI systems that are more rules-based and do not rely on machine learning are relatively explainable (see also discussion on *Technology Landscape: Artificial Intelligence*). Nevertheless, it was observed that documentation on such systems from technology developers remains lacking in detail and often does not explain the process of analysis followed by such technology tools, particularly when coupled with big data sets.

138. As AI systems, and machine learning in particular, continue to advance and are deployed, explainability will become an even more significant issue. The sheer volume of data being consumed by such advanced systems as input, together with their computational power to drive machine learning, leaves humans unable to keep pace with them or effectively oversee them using manual means. Systems matching these criteria already exist and firms and organizations are likely to need their own AI systems to test another AI system.

139. Lack of explainability is amplified in situations where the outputs of one AI algorithm becomes an input to another AI algorithm, creating a cascading effect.[156] Not only does this exponentially increase

---

[155] IAASB Digital Technology Market Scan: Natural Language Processing (June 2022) *https://www.iaasb.org/news-events/2022-06/iaasb-digital-technology-market-scan-natural-language-processing*

[156] See, for example, Nithya Sambasivan, Shivani Kapania, Hannah Highfill et al, "'Everyone wants to do the model work, not the data work'": Data Cascades in High-Stakes AI" (May 8, 2021) Google Research: https://storage.googleapis.com/pub-tools-public-

the potential for unintended consequences, but it also increases the probability that the system's "reasoning" cannot be explained by humans. Once again, this underscores the need for systems to be transparent and explainable.

140. Some approaches to developing transparent and explainable AI systems include:

- Developing systems that are more linear and transparent. Assessing the reasonableness of AI with an inferential approach (i.e., through the evaluation of inputs and outputs) only yields some level of comfort, as compared to the comfort gained from being able to explain an AI system that is linear and transparent.
- Embedding check points in AI machine learning processes. The more quality data that an intelligent agent has access to, the better and faster it learns. These check points could be in the form of logic and reasonableness tests conducted periodically (as frequently as multiple times per hour, depending on the volume of data ingested and speed of learning) for the human to understand what the intelligent agent is doing. It is also important to "pause" the learning of the intelligent agent during these check points.
- Ensuring that there is adequate documentation of the logic and rationale for the AI system's processing and decision-making. This is important so an independent third party, such as an auditor or regulator, can understand, explain, and validate the system. As mentioned previously, however, it is also observed that third-party technology is often inherently a "black box" because of challenges in obtaining access to source code, which is typically the intellectual property of the third party.
- Performing sensitivity analyses, for example, by altering a single input and measuring the change in model output. This gives a local, feature specific, linear approximation of the model's response. By repeating this process for many values, a more extensive picture of model behavior can be built up.[157]
- Model evaluation to validate that AI systems meet the intended purpose and functional requirements. For example, evaluation can be done by testing models on a "held-out" portion of the data (i.e., historical data inputs not used to train the AI), compare the model outputs with the actual, and report error.[158]
- Continuous evaluation by programming in "common sense" safeguards against outputs that clearly do not make sense by a large margin.[159]

---

publication-data/pdf/0d556e45afc54afeb2eb6b51a9bc1827b9961ff4.pdf and Karen Hao, "Error-riddled data sets are warping our sense of how good AI really is" (April 1, 2021) MIT Technology Review: https://www.technologyreview.com/2021/04/01/1021619/ai-data-errors-warp-machine-learning-progress/

157 Páez, A, "The Pragmatic Turn in Explainable Artificial Intelligence (XAI)", Minds and Machines, 29(3), doi: 10.1007/s11023-019-09502-w at 15: https://www.researchgate.net/publication/333390815_The_Pragmatic_Turn_in_Explainable_Artificial_Intelligence_XAI (page 451)

158 *Supra* note 44

159 *Supra* note 44

- Being aware of, and being able to identify and mitigate, inherent bias or incorrect assumptions used in the AI.[160] See discussion on *Objectivity: Bias*.

Responsibility for Transparency and Confidentiality

141. As trusted advisors, PAs bring credibility to information through exercising professional judgment and professional skepticism, among others. Given the increased level of uncertainty that comes with applying many emerging and disruptive technologies, in addition to the complexity of today's digital world overall,[161] the Working Group believes that it is important that PAs provide or communicate clear information in a straightforward manner to users of their services or activities about the limitations inherent in such services or activities,[162] and explain the implications of such limitations.[163] For example, this might include limitations of the technology employed, including the uncertainties inherent in it, related risks of unintended consequences, and the broader potential for ethics risks, including threats to a PA's compliance with the fundamental principles when employing such technology.

142. Providing such transparency around the challenges that PAs face in their different roles enhances public trust. Nevertheless, the level of transparency that PAs should aim for needs to be appropriate in the context and must continue to be bounded by the Code's fundamental principle of confidentiality, which requires a PA to respect the confidentiality of information acquired as a result of professional and business relationships.

143. Stakeholders observed that achieving the appropriate balance between transparency and confidentiality has sensitive and complex consequences for PAs which entail professional judgment. For example, if a PA determines that disclosure of non-compliance of laws and regulations to an appropriate authority is an appropriate course of action, they should also consider whether there would be legal protection in the particular jurisdiction if the PA overrides the confidentiality terms of their employment contract – this might warrant seeking legal advice. In addition, stakeholders highlighted the importance of recognizing that maintaining confidentiality is different from "secrecy" or "silence," which extend beyond professional confidentiality requirements. For example, stakeholders indicated that PAs need to have a clear "ethical rudder" to be aware of situations where information is deliberately controlled, withheld, or hidden to limit transparency under the premise of maintaining confidentiality.

144. Specific to technology, stakeholders noted that fully transparent technology, such as open-source software, can allow company leaders to have greater trust in the technology. It was suggested that source code visibility allows organizations to have a competent team analyze the code and its functionality. This would then enable the team to implement appropriate safeguards to assess that the code continues to function as intended and that the potential risks of its not doing so are identified.

---

160 See, for example, the challenges related to these issues in the results of a research study that found people both over-relied on the outputs from an AI system and misinterpreted what those outputs meant, even when they had knowledge about how AI systems work. Kyle Wiggers, "Even experts are too quick to rely on AI explanations, study finds" (August 25, 2021) VentureBeat: https://venturebeat.com/business/even-experts-are-too-quick-to-rely-on-ai-explanations-study-finds/

161 *Supra* note 133

162 Paragraph R113.3 of the Code

163 Proposed revised paragraph R113.3 of the Technology ED

Such visibility is seen as being similar to having access to a human team and interviewing them about their thought processes and decisions.

145. Stakeholders also observed that once there is a "trusted" logo on a technology tool or system, trust reliance is created (see discussion on *Objectivity: Over-reliance*). Therefore, it was stressed that in order not to mislead stakeholders, and to uphold the fundamental principle of integrity, the "trusted" technology provider (which could be a large professional firm) should be transparent and disclose the scope of its involvement with the technology. For example, stakeholders noted that such transparency and related disclosures would be useful to understand because they have observed instances where firm logos were marketed prominently alongside certain technology company logos even though the involvement of the firm was limited to the completion of a "demo" of a very specific component within the whole technology tool.

146. Finally, it was noted that organizations have varying levels of disclosures around non-financial matters, risk and corporate governance, etc. Stakeholders warned that too much disclosure can have the effect of making such information less useful. Transparency is considered useful and deemed to add value where it supports relevant decisions made by users of the information. So, the goal should be to match disclosures with decision making in an effort to produce better, and not simply greater, disclosure.[164] This translates into PAs striving to be transparent, motivated by a desire and intent to inform users and decision makers, while not releasing confidential information other than as permitted or required by law, regulation, or technical or professional standards.

Independence

147. When an individual PA, firm, or a network firm provides a non-assurance service (NAS) to an audit client,[165] they need to comply with the International Independence Standards contained in the Code.[166] 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[167] providing:

- NAS that involves assuming a management responsibility.
- NAS that creates a threat to independence that is not at an acceptable level and cannot be addressed by:

---

[164] For example, the IASB's current project on "Disclosure Initiative—Targeted Standards-level Review of Disclosures": https://www.ifrs.org/projects/work-plan/standards-level-review-of-disclosures/

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

[166] 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.

[167] 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.

- 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.

148. 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.

149. 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.

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

- 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).
- 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.
- 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

151. 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

152. 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.

153. 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.

154. 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 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.[168]

  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.

- 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.[169] A conflict might arise if the entity uses these tools to analyze data that later becomes subject to the firm's audit.[170]

155. 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 Client Data

156. As services are increasingly performed "online" by firms, many times this will 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,[171] 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

---

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

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

170 *[Placeholder for Ethical Leadership in a Digital Era: Applying the IESBA Code to Selected Technology-related Scenarios, anticipated to be release in Q4 2022.]*

171 Section 350 of the Code

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

157. 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.

158. 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

159. 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.[172] 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.

160. 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

161. 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.[173] 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

[172] 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.

[173] 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.

markets, and changes in technology. However, the conceptual framework and the general NAS provisions apply.

162. Stakeholder outreach suggested that a self-review threat might be created where a firm provides NAS[174] either through employing a technology tool or, more critically, selling or licensing a technology tool that performs the NAS.[175] 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 Technology ED sets out proposed revisions to explicitly clarify this matter.

163. 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.[176]

164. 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:

    - 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[177] to address the risk of a self-review threat, as such firms have fewer staff resources.

---

174 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.

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

176 *Supra* note 164

177 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.

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.

- 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.[178]

  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.

- 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.[179] 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.

- 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 entity is an audit client or will become an audit client in the future are important independence considerations in this regard.

- 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.

165. 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

[178] Paragraphs R400.30 to R400.32 of the revised NAS provisions

[179] Subsection 601 of the revised NAS provisions.

assurance on the outputs from such systems creates an independence issue.[180] The importance of appropriate safeguards[181] and transparency[182] 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

166. 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[183] 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. The Working Group notes that additional stakeholder feedback has been sought with respect to business relationships in both the IESBA strategy survey 2022 and the Technology ED, which will help inform possible future initiatives.

167. 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.

---

180 See proposed revisions to Part 4B in the Technology ED. The ED 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 News Release (June 2022): https://www.ethicsboard.org/news-events/2022-06/iesba-commits-readying-global-ethics-and-independence-standards-timely-support-sustainability

181 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?

182 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.

183 The Code defines a "close business relationships" and prohibits material close business relationships. The Technology ED also included additional examples of technology-related close business relationships.

D. Multidisciplinary Teams

Need for Multidisciplinary Teams

168. Given increasingly complicated technologies and complex systems, the need for multidisciplinary teams continues to grow to ensure appropriate design, development, use, governance, and control over technology.

169. As discussed in the subsection on *Competence and Due Care*, stakeholders stress that the traditional accounting, finance, or audit team needs to be complemented with diverse professionals from other disciplines to ensure the collective competence and due care is available for a PA to perform their professional activity. It was also observed that a PAIB's "value-add" within the larger team responsible for business strategy, finance and accounting, and IT, is frequently to act as a "bridge" between the IT and broader business groups. For example, PAs are effective at identifying appropriate key performance indicators to inform strategy, and the rationale for such choices, and can help guide technologists with respect to the tools needed to measure and monitor strategic implementation.

170. Stakeholders highlighted that, at a minimum, there needs to be an on-going and deep interdisciplinary engagement between PAs and technology professionals, even in situations where full multidisciplinary teams are not established. For example, a strong partnership is required between various business units under operations such as finance and accounting, human resources, and IT to ensure shared accountability for data governance and use.[184]

171. Finally, stakeholders see multidisciplinary teams as critical with respect to considering "who" is accountable when an issue occurs with a technology tool or system, particularly with the desire to increase PA involvement in developing, implementing, and operating innovative and transformative technologies. Multidisciplinary teams should also include various C-suite and management staff that are needed to enable an appropriate organizational ethics culture (e.g., tone at the top), and to promulgate this collective responsibility. This is seen as particularly effective in exhibiting to everyone in an organization, ethical behavior and adherence to appropriate policies and procedures.

The PA's Role on a Multidisciplinary Team

172. In the case of many large organizations, stakeholders cautioned that the influence of PAIBs is not currently perceived as "high" with respect to technology. Stakeholders also noted that PAIBs do not typically have the ability to impact technology adoption or development in a significant way. For example, when a company considers adopting or developing technology, data specialists and other IT specialists are typically the strategic advisors and drivers of such considerations, in addition to making up the implementation team. It was noted that PAs are rarely involved beyond performing KPI calculations, scenario analyses, or forecasting specific to the financial impact of the development and/or implementation. Stakeholders did, however, strongly encourage greater PA involvement. They suggested that PAs need to be part of the conversation on strategic value creation because of both their important bridging role across business units, particularly when serving in management and

[184] See also, for example, Thomas C Redman, "The Trust Problem That Slows Digital Transformation" (July 26, 2022), MIT Sloan Mgmt Review: https://sloanreview.mit.edu/article/the-trust-problem-that-slows-digital-transformation/

executive roles, and their business acumen, professional judgment, and adherence to the ethics principles of the Code.

173. For smaller organizations, on the other hand, stakeholders observed that PAs typically have a significantly larger role to play in IT strategy, driving the procurement or development and adoption of technologies within their organizations.

174. With the necessity of multidisciplinary teams in the digital age and a shift in public expectation for organizations to exhibit ethical decision-making more prominently (see discussion on *Why the Profession Needs to Act*), expectations of a PA's role within an organization and on multidisciplinary teams are changing. Specifically, stakeholders stressed the importance of PAs being able to manage such teams. At a minimum, PAs are expected to be involved in a greater range of issues and to raise related ethics concerns as they arise. To be effective in this regard, PAs should be involved from the start (i.e., when the strategic value creation conversations are occurring) so that ethics can be considered upfront. This includes ethics risk identification and management, such as implementing appropriate safeguards and governance structures (see discussion on *Ethical Leadership*).[185]

175. Stakeholders also remarked that automating accounting processes without a heavy PA involvement is not sustainable because it will lead to weaker internal control environments and, therefore, greater likelihood of data breaches, transactional inaccuracies, and reporting misstatements. See discussion on *Technology Landscape: Robotic Process Automation*.

Reliance on Experts

176. Data used as inputs for data analytics and other technology, use of emerging technologies (such as robotics, AI, and blockchain, among others), as well as managing cyber-security issues, are complicated, specialist areas. As a result, it is now very common to have IT specialists working closely with, or integrated within, traditional audit or accounting and finance teams. This creates an expectation that PAs need to have a broad sense of what the technology being used is doing, and understand when it is appropriate to scope technologists into their activities, and how best to do so.

177. Beyond just relying on such experts and their technical competence, expectations are emerging with respect to more formalized consideration of ethical values across the ecosystem of technology use, from scoping, development and implementation to operation and maintenance. However, the risk of blind reliance (knowingly or unknowingly) on technology experts by PAs was highlighted. It was acknowledged that the Code outlines the expectations for a PA in terms of:

[185] For PAs implementing AI in the financial services area, see for example, the IEEE's *Trusted Data and Artificial Intelligence Systems Playbook for Financial Services* (https://standards.ieee.org/industry-connections/ais-finance-playbook/), which includes best practice recommendations in this space.

- Determining whether a PA can rely on, or use, experts[186] (including consideration of conflicts of interest,[187] as well as independence requirements for engagement teams[188] and group audits);[189]
- Automation bias;[190] and
- Undue reliance on technology.[191]

E. Standards and Guidance

178. Stakeholders recognize the importance of the IESBA's efforts in developing consistent and clear standards for PAs with respect to ethics obligations across all PA roles.

179. Numerous suggestions were received around increased awareness raising, education, and implementation guidance for both PAs and non-accountants. Some of these comments and ideas are relevant for other standard setting, regulatory, and advocacy bodies (both internal and external to the accounting profession) to consider.

III. INSIGHTS AND RECOMMENDATIONS

180. This section outlines the Working Group's insights and recommendations arising from its analysis and evaluation process. The Working Group has aimed to identify which key themes and issues arising from its fact finding during stakeholder outreach and desk research have the potential to impact the Code or the IESBA's work more broadly. The Working Group's analysis and evaluation have been informed by input from the TEG and coordination with representatives of IAASB's Technology Initiative and IFAC's IPAE.

181. The Working Group's insights and recommendations are categorized into three broad groups, consisting of those that:

(a) Are technology-specific (Recommendations A to C);

(b) Have wider ethics relevance and application (including, but not limited to, technology) to the Code (Recommendations D to I); and

(c) Result in broader implications on the IESBA's work (Recommendation J).

These are each described in detail below.

---

186 Paragraphs 220.7 A1 and 320.10 A1 of the Code

187 Sections 210 and 310 of the Code

188 Glossary definition of "Engagement Team" of the Code

189 In February 2022, the IESBA released the *Exposure Draft: Proposed Revisions to the Code Relating to the Definition of Engagement Team and Group Audits* (ET-GA): https://www.ethicsboard.org/publications/proposed-revisions-code-relating-definition-engagement-team-and-group-audits. The IESBA noted that addressing the matter of independence for external experts is outside the remit of the ET-GA project but agreed to consider the matter as part of a future initiative.

190 Paragraph R120.12 A2 of the Code

191 Paragraph R112.1 of the Code

Technology-specific

A. Data Used for AI training

182. AI models need data to train on, and training on actual client or customer data provides the most effective and efficient training. As a result, it is becoming more common for firms and companies to want to use anonymized client or customer data to train AI models to enhance or improve audit quality, business insights, and the efficiency and sustainability of internal processes.

183. The use of such data to enhance internal, firm-wide or organizational functions is seen by some stakeholders as akin to PAs taking their "lessons learned" of the past and applying the learning to their next project or task. What is different is that now the "lessons learned" are being applied by the AI model instead. As technology allows us to use data in a more cohesive way, such "learning" has increased the challenges when identifying, evaluating, and addressing threats to compliance with the fundamental principles of integrity and confidentiality (which also existed in the non-digital environment):

- A lack of transparency to clients or customers about the use of their data, even if anonymized, might be a breach of R111.2(c),[192] which requires the PA not to be associated with information that is misleading through omission or obscurity.

  In this regard, the Working Group notes that PAs can apply safeguards – such as obtaining consent from the client or customer whose information is being anonymized and used for the AI training – in order to reduce the threat to complying with the fundamental principle of integrity to an acceptable level.

- R114.1(e)[193] specifies requirements for maintaining confidentiality, and explicitly states that confidential information cannot be used for the personal advantage of the accountant or for the advantage of a third party (which would include the firm or employing organization). In addition, R114.1(f) states that any confidential information cannot be used or disclosed after a professional or business relationship has ended. These requirements might lead users of the Code to believe that the use of client/customer data, whether anonymized or otherwise, to train internal AI systems would be prohibited, even with consent.

  The Working Group recognizes that there is a public interest benefit regarding the use of real client or customer data, with consent, for the purpose of enhancing firm- or organization-wide functions. This public interest benefit should be considered alongside the evaluation of threats to confidentiality and integrity.[194]

184. **Recommendation A: Revise the Code, for example, in Subsection 114 *Confidentiality*, to clarify whether firms and organizations may use client or customer data for internal purposes, such as training AI models, and if so the parameters of such use (prior, informed consent; anonymization). Non-authoritative guidance should also be developed to specifically**

[192] "… A PA shall not knowingly be associated with reports, returns, communications or other information where the accountant believes that the information: … Omits or obscures required information where such omission or obscurity would be misleading."

[193] "… An accountant shall 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. …"

[194] Further commentary on some of the risks associated with training AI systems using "real" data are included in a meta-analysis of AI ethics guidelines implementations by Thilo Hagendorff, "The Ethics of AI Ethics: An Evaluation of Guidelines" (2020) *Minds and Machines* 30:99-120, online: https://link.springer.com/article/10.1007/s11023-020-09517-8

emphasize the expectations for complying with the fundamental principle of integrity when using client or customer data for AI training, i.e., obtaining consent that is meaningful, informed, and transparent.

185. The Working Group notes that the IESBA's Technology ED has proposed revisions to Section 114 on Confidentiality, though not with respect to this specific issue.

B. Transparency and Explainable AI

186. The decision-making processes or rationale of an AI system might not be explainable or understood by a human[195] (i.e., the system might operate as a "black box" process). Some types of machine learning are more prone to the development of AI systems that are less inherently explainable.[196] As AI systems become more sophisticated, complex, and autonomous, there is a heightened need for AI to be explainable, to allow for sufficient human oversight.[197] Accordingly, transparency and explainability in support of a PA's public interest responsibility will become even more important as technology developments rapidly advance, for example, as the realm of "cognitive AI" emerges.

187. In the business world, decisions can very broadly be categorized as low- or high-risk, based on the significance of the economic and/or social impacts. The use of AI for relatively low-risk automated decision-making might be a commercially optimal approach. On the other hand, the use of AI for high-risk decisions, such as decisions in the public sector around social programs, diagnostic decisions in healthcare, and safety-critical systems in autonomous vehicles, requires more scrutiny.[198] In these high-stakes contexts, a single decision might have significant economic, business, social, or human impacts. The higher the stakes, the more important it is that the AI be explainable in order for humans to have appropriate oversight of decisions being made. Such oversight would not be possible without the system being adequately explainable. Regulators and multilateral organizations have begun recognizing this need for greater consistency and oversight. For example, see the UNESCO *Recommendation on the Ethics of Artificial Intelligence*[199] and the proposed EU *AI Act* referenced in the section above on *Technology Landscape: Artificial Intelligence*.

188. The Working Group also notes that the concept of understanding AI (which implicitly means AI must be "explainable") is outlined in non-authoritative guidance issued by IAASB staff on the *Use of Automated Tools and Techniques When Performing Risk Assessment Procedures in Accordance with ISA 315 (Revised 2019)*.[200] For example, in an AI (machine learning) environment, the FAQ highlights the importance of an auditor:

- Considering the algorithms embedded in, and the learning by, the AI.

---

195 The terminology in this area is still somewhat dynamic, and might refer to concepts such as explainable AI, understandability, interpretability, explicability, etc.

196 *Supra* note 44

197 *Ibid.*

198 *Ibid.*

199 *Supra* note 44

200 Question 5: "…the auditor may need to consider the algorithms embedded in, and the learning by the AI as a complement to the human thinking and decision-making process. As such, the auditor's understanding of how the creation and modification of the algorithms operating are controlled and maintained may be important."

- Understanding how the creation and modification of the algorithms are controlled and maintained.

The IOSCO has also published guidance for intermediaries and asset managers using AI and machine learning that highlights several areas where potential risks and harms may arise in relation to the development, testing, and deployment of solutions incorporating such technology.[201] Transparency and explainability are among the six areas highlighted, and although the guidance is not directed at PAs and firms, it illustrates that the topic area has gained significant regulatory attention.

189. **Recommendation B: Develop further guidance around the importance of transparency and explainability, whether through non-authoritative guidance or in the Code, specific to when a PA relies on or uses transformative technologies (e.g., AI). Such guidance would highlight that PAs cannot abdicate their public interest responsibility and accountability when relying on or using technology (even in highly automated environments).**

190. **This additional guidance might explicitly set out expectations for a PA when relying on a technological solution. For example, before relying on a machine learning tool, the PA would be expected to ensure that the tool is explainable (i.e., that they can reasonably understand the rationale for decisions made by the technology). The Working Group believes that the PA need not be the expert who can explain the tool, but should have access to such an expert and should obtain a reasonable understanding in order to be comfortable with the tool's inputs, processing, and outputs.**

191. **Furthermore, consideration should be given to the ethics expectations for PAs when they are involved with developing transformative technology solutions, for example that they be expected to promote the development of explainable systems, particularly in high-stakes applications.**

192. The Working Group notes that the Technology ED includes proposed factors for PAs to consider when determining whether to rely on, or use, the output of technology.[202] The ED also contains proposals to strengthen expectations around a PA's obligation to be transparent to users of the PA's professional activities or services.[203] The Working Group also notes the IESBA's explanation of how the concepts of "transparency" and "explainability" are covered in the proposed revisions to the Code (paragraph 36(b) of the explanatory memorandum to the ED).

C. Data Governance, including Custody of Client Data

193. Recognizing that data is key to driving the effective application of technology, the Working Group believes that it is important for PAs to recognize that they have strategic value in data governance

---

[201] IOSCO, *The use of artificial intelligence and machine learning by market intermediaries and asset managers: Final Report* (September 2021): https://www.iosco.org/library/pubdocs/pdf/IOSCOPD684.pdf

[202] Proposed paragraphs 220.7 A2 and 320.10 A2 of the Technology ED include considerations about the PA's ability to understand the output from the technology for the context in which it is to be used, and the employing organization's or firm's oversight of the design, development, implementation, operation, maintenance, monitoring or updating of such technology.

[203] Proposed revisions to paragraph R113.3 extend a PA's obligation to be transparent by proposing that the PA also provide users (of the professional services or activities a PA undertakes) with sufficient information to understand the implications of limitations inherent in such services or activities.

and management (including cybersecurity implications). For example, a discussion paper[204] proposing a data management value chain[205] was jointly released by IFAC and CPA Canada in April 2021 to capture how the expertise of accountants can be applied in four different areas – as data engineers,[206] data controllers,[207] data scientists,[208] and strategic advisors.[209] Commentators on the discussion paper largely provided suggestions around the development of non-authoritative educational material so that PAs can be appropriately upskilled and made aware of the expectations around data governance.[210]

194. Furthermore, the Working Group notes that holding client data is becoming increasingly common among firms. Data created or collected is not recognized as an asset under current financial reporting standards. However, there is consensus that if data is lost, misappropriated or misused, or subject to unauthorized access (including, for example, a breach of privacy), then there is – at the very least – a reputational loss, if not financial and legal consequences, to the organization or firm. For example, it is noted that:

> *…many, if not most, accountants continue to appreciate the fact that data reflects the characteristics of a financially reportable asset because it has a probable future economic benefit… For some, data is something that is either loaned temporarily to accountants so that they may use it to create something of value for its owner, like a liability. Still others believe that the accountant's role as it relates to data is a custodial one; the owner trusts the accountant with information, and the accountant implements appropriate due care controls that ensure the data's protection.*[211]

195. In this regard, the Working Group notes that Section 350 of the Code addresses custody of client assets but does not explicitly contemplate custody of client data.[212] Data is the foundation of all financial and non-financial (e.g., sustainability) reporting, and impacts both PAPPs as well as PAIBs. For this reason, the Working Group believes that ethics considerations with respect to the custody of client data should be broader in scope than data underlying financial reporting or internal controls over financial reporting, and extend to all PAs.

196. **Recommendation C: Revise the Code to address the implications of a PA's custody or holding of client data. Such a workstream could be scoped to also include considering threats to**

---

[204] IFAC and CPA Canada: The PA's Role in Data – Discussion Paper (April 2021) https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/publications/professional-accountants-role-data

[205] IFAC: Data and the Future-Fit Accountant (May 2021) https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/data-and-future-fit-accountant

[206] To ensure data has integrity, is clean and reliable in the data gathering phase

[207] To ensure the stewardship of data resources in the data sharing phase in the same way as the existing controllership role covers the stewardship of financial and physical resources

[208] To provide insights through the analysis and interpretation of complex data to support decision-making

[209] As an effective communicator, analyzing and explaining complex business issues within a local, national or global context based on the strengths and limitations of the data, and on the assumptions and models that underpin derived insights

[210] As such, following this, a webinar was arranged in this regard, see Data Management Value Chain: An Opportunity for Accountants in the Digital Age.

[211] CPA Journal: Managing Data as an Asset (June 2019): https://www.cpajournal.com/2019/06/24/managing-data-as-an-asset/

[212] To enable more information gathering, the IESBA determined in June 2021 that the "custody of client data" by a PAPP in a non-audit context is not in the scope of its current Technology Project.

compliance with the fundamental principles given the complexity created for PAs who need to remain current with an evolving patchwork of cross- and intra-jurisdictional data privacy laws and regulations, as well as the ethics challenges related to data governance and management (including cybersecurity).

197. **Continue raising awareness of a PA's strategic role in data governance and management (including cybersecurity), and develop educational resources to highlight such role.**

Insights With a Wider Ethical Relevance and Application, Including Technology

D. Ethical Leadership and Decision-making

198. Technological innovations are increasingly being developed, applied, and commercialized to enhance efficiencies, insights, and profits within professional and business services. In this context, stakeholders noted that there are instances where developing, implementing or using technology raises questions about the extent to which ethics-related issues are considered in decision-making.[213] Examples include considering:

- Threats of data misuse and to privacy, and security.
- The risk of social harm.
- Bias in the outputs of technology, such as AI.
- Inadvertently spreading mis- or disinformation.
- A lack of effective human oversight and acceptance of responsibility over unintended consequences arising from technology.

These have the potential to threaten the PA's compliance with the fundamental principles.

199. The Working Group notes a PA's responsibility[214] to act in the public interest under the Code, as well as the expectation for PAs to encourage and promote an ethics-based culture in their organizations, taking into account their position and seniority.[215] This expectation to exhibit ethical leadership and decision-making extends across every industry and role that PAs work in, as well as to emerging forms of technological innovation that might underpin such work. Understanding the underlying economic substance and commercial purpose of transactions or business models (including those being conducted with, or through, technology such as e-commerce, cloud-based transactions, etc.) is important to enable PAs to act in the public interest.[216] Accordingly, it is crucial that PAs are "at the

---

213 Note that these questions around ethics do not necessarily represent concerns related to falling foul of laws or regulations, i.e., not rising to the level that would trigger the Code's provisions on responding to non-compliance with laws and regulations (NOCLAR).

214 The Code outlines a PA's responsibility for ethical leadership in terms of holding themselves and their organizations accountable for ethical decision-making in the public interest (see paragraphs 100.1, R100.6 and 100.6 A1). The Working Group notes that this is inclusive of decisions regarding the responsible development, implementation, and use of technology. In this regard, the Working Group also notes the proposals contained in the Technology ED that are intended to guide the ethical mindset and behavior of PAs as they deal with changes brought by technology in their work processes and the content of the services they provide.

215 Paragraph 120.13 A3 of the Code

216 See, for example, IESBA June 2022 Meeting Agenda Item 5: Tax Planning & Related Services: https://www.ifac.org/system/files/meetings/files/Agenda-Item-5-Tax-Planning-and-Related-Services-Jens-Poll.pptx

table" when decisions are being made about the development and use of technology, especially in situations where there is a potential for unintended consequences. See discussion on *Key Themes Observed: Public Interest Accountability of PAs*.

200. The Working Group and stakeholders noted that this responsibility for ethical leadership in all roles that PAs are involved in includes, but also extends beyond, the issues raised by technological innovation, and is common to all types of complex situations. As such, the consideration of how the profession should respond is a matter that should not be limited to the context of technology – a holistic approach will likely be more effective.

201. **Recommendation D: With a view to the broader expectations[217] for PAs to exhibit and champion ethical leadership and decision-making, develop non-authoritative guidance to emphasize the potential actions a PA might take when applying the conceptual framework and complying with the Code's fundamental principles in technology-related scenarios relevant across various PA roles and activities.[218]**

202. The Working Group also believes that the IESBA can leverage the opportunities offered by its ongoing workstreams to further emphasize such expectations, for example, by collaboration among the:

- *Tax Planning and Related Services* Task Force, which is developing an ethics framework to aid PA decision-making in situations pertaining to tax planning. The Working Group believes such a framework can have broader applicability;
- Sustainability Working Group, which is developing a strategic vision to guide the IESBA's standard-setting actions in relation to sustainability reporting and assurance, given this domain's considerable potential for ethical issues that PAs will need to manage; and
- Planning Committee, which is initially considering the responses to the Strategy Survey 2022 that requested stakeholder views on whether the IESBA should dedicate strategic focus on further raising the bar of ethical behavior for PAIBs in its next strategy period (2024 to 2027).

In this regard, the Working Group can provide further input, as relevant, on identified technology-related implications.

E. Communication with Those Charged With Governance

203. Stakeholders increasingly observe that when technology is used or relied upon, there might be an "outsourcing," or the perception of "outsourcing" by a reasonable and informed third party, of responsibility for oversight to the technology provider or an external consultant, resulting in a potential lack of appropriate due care, competence, and objectivity. For example, when a PA relies on an external expert or consultant to develop or implement technology, or to provide advice on a technology-related issue (e.g., cybersecurity risks), such reliance is sometimes treated as a "silver

---

[217] Proposed revision to the Code in the Technology ED, paragraph 120.13 (b), explicitly broadens this expectation to business organizations and individuals with which the PA has a professional or business relationship.

[218] See, for example, the CPA Canada, ICAS, IFAC & IESBA series on "Ethical Leadership in the Digital Age:" https://www.ifac.org/knowledge-gateway/building-trust-ethics/discussion/ethical-leadership-digital-age and *[placeholder for Ethical Leadership in a Digital Era: Applying the IESBA Code to Selected Technology-related Scenarios, anticipated to be released in September Q4 2022.]*

bullet"[219] or used as rationale by the PA to minimize their own responsibility for overseeing the technology or issue.

204. **Recommendation E: To strengthen the concepts of transparency and accountability, add new material to the Code as part of the subsections on "communication with TCWG" in Parts 2 and 3 to encourage, or require, meaningful communication[220] with TCWG by PAs (including individual PAPPs and firms)[221] about technology-related risks and exposures that might affect PAs' compliance with the fundamental principles and, where applicable, independence requirements.**

205. Technology-related communications could, for example, include information on:

- The nature of the activity to be performed by the technology, and how the PA has determined that such technology is effective for the purpose intended.
- Any limitations in understanding or explaining the technology, in particular how such limitations might affect acting with sufficient expertise, training, or experience.
- The nature and scope of a technology expert's service, if such expertise is sought and relied upon or used, and the plan for managing and monitoring the system in the future if the expert's service is a limited term engagement.
- Any potential conflicts of interest, such as whether the technology expert being relied upon has a self-interest in recommending a particular technology or implementation approach.
- Any threats to the fundamental principles and, where applicable, independence, that have been identified in relation to the use of, or reliance on, technology or a technology expert, the basis for the PA's assessment that the threats are at an acceptable level or, if not, the actions the PA will take to eliminate or reduce the threats to an acceptable level.

Strengthening such communication provisions in the Code could, in particular, make it explicit where the responsibility for oversight of developing, implementing, or using technology lies (i.e., including PAs and IT professionals, such as data scientists, technologists, and engineers). For example, this would make it clear to TCWG who is in charge of, and accountable for, each specific process or function. This will be beneficial given the increasing inter-disciplinary interactions, complexity, and

---

219 For example, the US Public Accounting Oversight Board (PCAOB) in its publication on 2021 Conversations with Audit Committee Chairs notes that: "One recurring idea that we heard from audit committee chairs is that emerging technologies, despite all their promise, may never be a silver bullet. One audit committee chair, for example, expressed the view that emerging technologies should be thought of as supplemental tools. Another suggested that reliance on technology may be just the opposite of a silver bullet, to the extent that it dulls auditors' ability or inclination to incorporate their business insights into procedures."

220 For example, in the US PCAOB's publication on 2021 Conversations with Audit Committee Chairs, it was highlighted that "one [audit committee] chair added appreciation for the auditor's ability to explain how technology can be used to identify risk areas and to make the audit more effective."

221 The Working Group notes that the IESBA's current strategy and work plan (2019 to 2023) had considered whether strengthening the provisions in the Code regarding communication with TCWG would promote stakeholder confidence in the audit profession. At the time, the IESBA determined not to prioritize it given the relatively low support among respondents for this topic. The IESBA determined instead to direct its NAS Task Force to address the specific matter of communication with TCWG in the context of NAS. In this regard, the revised NAS provisions set out the new provisions regarding communication with TCWG in relation to NAS.

sophistication arising from the development, implementation, and use of disruptive and transformative technologies.

206. The Working Group acknowledges that communication with TCWG around identifying and evaluating threats to compliance with the fundamental principles arising from specific facts and circumstances, and the actions or measures taken to eliminate or reduce those threats to an acceptable level, could apply to all professional activities or services that a PA may perform (i.e., this is not unique to the use of, or reliance on, technology, but could also be relevant for sustainability reporting, tax planning, etc.).

F. Reliance on, or Use of, Experts

207. Preparing and presenting financial and, in particular, non-financial information (e.g., sustainability information) typically involve the assistance of, or reliance upon, technology experts. The question arose as to the factors PAs should consider when gaining confidence that a technology expert can be trusted and relied-upon to make ethically appropriate decisions (i.e., that are in alignment with the Code's ethics principles), and to what extent the Code could serve as the basis for an evaluation approach.

208. Stakeholders acknowledged that this is not a new question and represents a matter of professional judgment when applying extant Sections 220 and 320. Several suggested, however, that more explicit consideration of the ethics across the decision-making ecosystem would be beneficial in enhancing the reliability of information prepared and presented. This would also support the resultant decisions made, given the increasing complexity of various subject matters that require a multi-disciplinary approach and reliance on third-party specialists (i.e., deploying advanced technologies, sustainability, valuations, tax planning, etc.).

209. A few stakeholders went so far as to recommend that consideration be given as to how the Code might be made more relevant and applicable to others in the ecosystem who are not PAs.

210. **Recommendation F: Develop non-authoritative guidance and/or revise the Code in paragraphs 220.7 A1[222] and 320.10 A1[223] to emphasize the importance of a PA assessing the extent to which an expert being used and relied upon behaves in alignment with the Code's fundamental principles, and the factors to consider in making such an assessment.**

211. The Working Group notes that this matter of "experts" is significantly broader than just technology experts. It is also particularly relevant in other emerging PA activities, such as sustainability reporting.

212. The Working Group also believes there is an opportunity for the Code (or parts of it) to be applied by professionals other than PAs. In this regard, the Working Group acknowledges that the IESBA Strategy Survey 2022 is actively seeking stakeholder feedback on exploring the question of whether the public interest would be served if, for example, the scope of the Code were enlarged to permit its

---

[222] Factors to consider in determining whether reliance on 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.

[223] 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.

applicability in relation to sustainability assurance services provided by professionals other than PAPPs.

G. Threshold for "Sufficient" Competence

213. As noted in the discussion of the Competence theme above, there is an ongoing need for continuous upskilling resulting from the pace of change in technology. Recognizing this general need to upskill for all PAs, stakeholders commented on and questioned what competence threshold should be considered as "sufficient" in today's complex, dynamic, and uncertain world. The general consensus is that PAs need to be well enough versed to ask appropriate questions to identify and manage the risks and take advantage of the opportunities related to innovative and transformative technologies, but that mastery of specific technologies by all PAs would be neither necessary nor realistic.

214. **Recommendation G: Engage more actively with other bodies, such as IFAC's International Panel on Accountancy Education (IPAE) and PAOs, to encourage them to arrange educational activities to raise awareness about the characteristics of "sufficient" competence in the context of the Code and the International Education Standards (IESs). Such other bodies are better placed to develop non-authoritative guidance to illustrate and emphasize how the Code's principles apply when determining sufficient competence.**

H. Pressure on PAs

215. Concerns continue to be heard regarding pressures faced by PAs due to:

- Information overload.
- Pace of change in technology, laws, and regulations, etc.
- Time pressures that threaten the ability to effectively understand and/or assess the reasonableness or appropriateness of using technology.
- Organizations seeking to find the "silver bullet" technology to achieve performance targets, including automation and AI.

In discussions with stakeholders, these pressures are sometimes framed as PAs feeling intimidated, but often not in the typical sense described in the Code now. The "intimidation" can come from a sense of being legitimately overwhelmed by the technology (including simply not possessing the capacity to understand the technology, a lack of time, or the pace of change), rather than based on pressure exerted by another individual.[224]

216. These drivers of pressure on PAs are aligned with the "elements of complexity" that respondents highlighted as part of the IESBA's 2020 global survey on Complexity and Technology in the Professional Environment (the results of which were considered in the Technology Project).[225] In

[224] In the broader sense, this "overwhelm" is sometimes discussed in the context of burnout and other mental wellness issues. For example, a recent CPA British Columbia survey found that CPAs were more likely than other workers to feel physically and/or mentally exhausted after finishing their workday. See Jamie Midgley, "Mental wellness in the CPA profession" (May 5, 2022) CPA BC News: https://www.bccpa.ca/news-events/latest-news/2022/may/mental-wellness-in-the-cpa-profession/

[225] The Technology ED includes a discussion of complex circumstances and provides guidance to help PAs manage these complex circumstances and mitigate the resulting challenges.

setting the scope of the Technology project, the IESBA determined at the time not to encapsulate such elements in a new category of threat nor modify an existing category of threat.

217. For now, in response to the continued stakeholder concerns about the pressure felt by PAs, the Working Group has contributed and provided input to non-authoritative resources that highlight such pressure on PAs. For example:

- Ethical Leadership in an Era of Complexity and Digital Change: Paper 1 – Complexity and the professional accountant: Practical guidance for ethical decision-making, released in August 2021.
- Exploring the IESBA Code – A Focus on Technology: Artificial Intelligence, released in March 2022.
- *[Placeholder for Ethical Leadership in a Digital Era: Applying the IESBA Code to Selected Technology-related Scenarios, anticipated to be release in Q4 2022.]*

218. **Recommendation H: Revise the Code, for example within Section 270 *Pressure to Breach the Fundamental Principles*, to include illustrations of pressures on PAs (such as time and resourcing constraints; competence gaps; complexity of technology, laws and regulations; pace of change; uncertainty, etc.). In addition, consider revising the description of the intimidation threat (paragraph 120.6 A3)) to encompass this broader manifestation of pressure beyond that exerted by another person.**

219. **In addition, advocate to PAOs and other bodies, such as IFAC's IPAE, the development of additional non-authoritative resources to raise awareness of, and provide guidance on, how PAs can manage sustained pressures.**

I. Business Relationships

220. The profession is seeing a rise in strategic and commercial relationships (often referred to as "alliances," "partnerships," or "ecosystems") between accounting firms and technology and other companies. Whereas Section 520 *Business Relationships* addresses "close business relationships" between an audit firm and an audit client or its management, such as through joint ventures or combining products or services, it does not address broader business relationships.

221. **Recommendation I: Given the rise in strategic and commercial relationships between accounting firms and technology and other companies, revise Section 520 *Business Relationships* more comprehensively to address potential threats to the fundamental principles and, where relevant, independence, in the context of broader business relationships and new forms of relationships that are emerging.**

222. The Working Group notes that the Technology ED considers situations where a firm and a technology company co-develop and market a product together for their clients, which do not include the firm's audit clients.[226] However, the Working Group believes that the issue is broader than the current Technology project's scope because:

(a) The situation becomes more complicated where such product might then be "on-sold" to the client's customers, which might include one or more of the firm's audit clients. The Working

[226] Proposed revisions to paragraph 520.3 A2 (last bullet) of the Technology ED

Group believes there is merit to highlighting this risk of self-review threat down the line and further information gathering as to how firms currently manage such broader downstream risk; and

(b) As these types of relationships continue to rise, there is greater potential for the emergence of other threats to complying with the fundamental principles. This warrants closer consideration.

One example provided by stakeholders included where a firm's logo was marketed prominently alongside a technology company's for a software product, even though the involvement of the firm was limited to a very specific component within the considerably more comprehensive product being marketed by the company. Such marketing might mislead purchasers or licensees of the tool to believing that the application has been appropriately tested by the firm, resulting in an immediate "trust" or over-reliance on the tool.[227] The Working Group believes that increased transparency and related disclosures would be useful to better understand the nature and extent of the relationship between the firm and the technology or other company.

223. The Working Group also notes that the concept of threats to independence from broader business relationships has been included in the IESBA Strategy Survey 2022, where stakeholders have been requested to rate the importance of this topic as a strategic priority for the IESBA's 2024 to 2027 strategic work plan.

Insights Resulting in Broader Implications on IESBA's Work

224. The Working Group notes that the key themes in Section II also have broader implications pertaining not only to the IESBA, but also to its stakeholders (including regulators and other standard-setters, as well as PAOs, firms, and academics) in the broader ecosystem.

225. **Recommendation J: Continue initiatives to:**

- **Advocate the importance and relevance of Code: PAs are bound by the requirements of the Code, but the Working Group observed that some stakeholders exhibited a lack of awareness of the Code's fundamental principles, conceptual framework, and a PA's duty to act in the public interest.**

  The Working Group believes that it is therefore of utmost importance for the IESBA to further raise awareness of the Code, which enables PAs to fulfil their professional responsibility to act in the public interest, and promote reference to the Code by other standard-setters and regulators.[228] This, of course, requires other such bodies and stakeholders – such as TCWG and investors – to recognize the importance of high standards of ethical behavior. It is also important that they recognize the role and contributions of the Code to guide ethical decision-making in the public interest and to meet the organizational and market needs for trustworthy financial and non-financial information.

[227] See paragraph 145

[228] For example, to enable the enforcement of the Code by jurisdictional regulators, and where regulators already enforce the Code, to help promote its consistent enforcement

To drive this, the IESBA and its representatives should further engage with other bodies to advocate for[229] how and why the Code is increasingly relevant in today's environment. This would also help promote greater involvement by PAs at more diverse decision-making tables. This is because PAs can demonstrate not only ethical behavior, but also assist in driving the ethical design, implementation, and use of technology solutions.

- **Develop, facilitate the development of, and/or contribute to non-authoritative resources and materials: Rapid advancements in technology, its applications and related issues mean that the continued development and release of practical application guidance based upon the provisions of the Code is critical, especially in relation to important emerging issues.**

  The Working Group believes that to enable agility, speed to market, and fit-for-purpose guidance, issuing non-authoritative resources and materials is best done in collaboration with other stakeholders, rather than by the IESBA alone.

  To this end, the Working Group has summarized for the IESBA and other stakeholders (i.e., IFAC, PAOs, NSS, and other standard-setters), the pertinent technology-related topics that would particularly benefit from additional non-authoritative guidance to draw out potential ethics issues that might arise and how the Code applies in such scenarios.

  These suggestions are presented as Appendix II.

226. The Working Group further believes that the effective undertaking and execution of such initiatives will support and promote the timely adoption and effective implementation of the Code, which is aligned with the proposed fourth strategic focus for the IESBA's next Strategic Work Plan (2024 to 2027).

IV. SUGGESTIONS FOR THE FUTURE OF THE IESBA'S TECHNOLOGY INITIATIVE

227. Reflecting on the substantive stakeholder outreach, desktop research, and other activities undertaken by the IESBA during both Phase 1 (2019-2020) and this second phase (2021-2022) of its fact-finding; the Working Group notes that the key themes observed have become increasingly consistent over time. The broad insights gathered also remain relevant despite the different types of technology being assessed and evaluated.

228. Specifically, the technology landscape, although dynamic and evolving, has not seen a revolutionary turn that would significantly impact the relevance of the Code as of 2021 (including revised NAS provisions). Rather, the findings of Phase 2 underpin the fact that, with few exceptions, the Code (including revised NAS provisions) continues to remain applicable and relevant to guide ethical decision-making around a PA's involvement with the design, implementation, or use of disruptive and transformative technologies and related issues. The expected finalization of the proposed technology-related revisions to the Code in early 2023 will additionally enhance the Code's robustness and expand its relevance in this environment. Also, the IESBA's careful consideration of the Working Group's Phase 2 recommendations, in the context of its other workstreams and future

[229] For example, the Working Group notes the IESBA's letter to the International Sustainability Standards Board (ISSB) in this regard.

strategic priorities, will help ensure that the Code's continued relevance into the future as technology reshapes the roles PAs undertake.

Four-pillar Approach

229. Nevertheless, it is clear that technology is not "one and done" and that innovations of technology should continue to be monitored by the IESBA. As such, the Working Group suggests a four-pillar approach for the IESBA to consider, with a re-evaluation in December 2023:

- **Pillar 1:** Making available regular internal education for the Board on emerging areas, such as technology and sustainability.

  Proposed approach: The Working Group suggests that the relevant workstream on the subject matter (such as through the Technology Working Group and Sustainability Working Group) is well-positioned to arrange such internal education opportunities in this regard. This includes suggesting appropriate timing and relevant subject matter experts.

- **Pillar 2:** Conducting ongoing, but substantially less intensive, environmental scanning to monitor advancements and developments in existing and new technologies, their application, and related issues.

  Proposed approach: The Working Group suggests that the TEG continue to provide input to the Working Group in this regard and that for 2023 two environmental updates be obtained from the TEG and shared with the Board.

- **Pillar 3:** Maintaining the capacity for ad hoc analysis of technology-related issues encountered by IESBA workstreams, to identify and assess any potential Code implications or need for additional non-authoritative guidance.

  Proposed approach: The Working Group believes that it, supported by the TEG, is well-positioned to continue its remit in this regard.

- **Pillar 4:** Maintaining the capacity for engagement with other IESBA workstreams or non-IESBA stakeholders to facilitate the consideration of the Phase 2 recommendations, as well as contributing to the development and/or review of non-authoritative resources and materials outlined in Appendix II.

  Proposed approach: The Working Group believes that it, supported by the TEG as needed, is well-positioned to provide input in this regard. This is because the Working Group is well versed in the key themes and insights and recommendations arising from the initiative's findings.

The Working Group further notes that this suggested four-pillar approach is similar to the IAASB's approach with respect to its own technology initiative.

APPENDIX I: SUMMARY OF OUTREACH, EVENTS, PRESENTATIONS AND PANEL DISCUSSIONS

Appendix I presents a summary of the Working Group's key fact-finding activities with stakeholders which informed this report. For easy reference, the activities have been grouped into:

- Input from the Technology Experts Group
- Targeted outreach with stakeholders
- Presentations from external parties
- Panel discussions
- Emerging technologies conference

This appendix also presents a one-page summary table.

Input from the Technology Experts Group (TEG)

1. The IESBA TEG acts as a "sounding board" to the IESBA's Technology Working Group, providing advice and other input that helped inform the Working Group's fact-finding work and deliverables. The Working Group met on three occasions with the TEG since the TEG's establishment in March 2022.
2. The TEG is chaired by IESBA Member and Chair of the Technology Working Group, Mr. Brian Friedrich. TEG members are experienced in using and implementing technology:
    - Jason Bradley, Financial Reporting Council, United Kingdom
    - Mary Breslin, Verracy, North America
    - Danielle Cheek, MindBridge AI, North America
    - Muhammad Fahad Riaz, Maglytic, Middle East
    - Clinton Firth, Ernst & Young, Middle East and North Africa
    - William Gee, PricewaterhouseCoopers, Mainland China and Hong Kong
    - Loreal Jiles, Institute of Management Accountants, North America
    - Mario Malouin, Innovators Alliance, North America
3. These stakeholders have experience either working in organizations with a global reach and impact, or that is specific to a jurisdiction. The jurisdictional regions covered Africa, Asia-Pacific, the Middle East, Latin America, North America, Europe and the UK.

Targeted Outreach with Stakeholders

4. In developing this report, the Working Group considered a balanced and diverse set of perspectives, professional and business roles and experiences from a variety of stakeholders through its targeted outreach including with individuals representing those charged with governance, investors, regulators, public sector and oversight bodies, technologists (software vendors and developers) and PAIBs, PAOs including NSS, and accounting firms and PAPPs. Specifically, this extended to a

diverse range from at least 31 individuals, in addition to a number of individuals participating in 6 group workshop events.[230]

5. These stakeholders either have experience working in organizations with a global reach and impact, or that is specific to a jurisdiction. The jurisdictional regions covered Africa, Asia-Pacific, the Middle East, Latin America, North America, Europe and the UK.

6. Such targeted outreaches are listed below, in no particular order:

   TCWG, including corporate governance and ethical AI and data governance advocacy bodies

   - Global Network of Director Institutes (GNDI) and Institute of Corporate Directors, Canada (ICD) – Rahul Bhardwaj, GNDI Chair and ICD (Canada) CEO.

     GNDI is a global network representing more than 150,000 directors, which is focused on enhancing the capability of directors to drive sustainable performance for the benefit of shareholders, the economy and society) and CEO of the ICD in Canada.

   - MindBridge AI – Eli Fathi, Chair of the MindBridge Board and former MindBridge CEO.

     MindBridge develops AI software that, through the application of machine learning and artificial intelligence technologies, helps organizations across multiple industries (including audit firms) detect anomalous patterns of activities, unintentional errors and intentional financial misstatements.

   - Asian Corporate Governance Association (ACGA) – Jamie Allen, Secretary General; Nana Li, Research and Project Director. Jamie is a former member of the Financial Reporting Review Panel and Hong Kong Stock Exchange listing committee.

     ACGA is a non-profit membership organization dedicated to working with investors, companies and regulators in the implementation of effective corporate governance practices throughout Asia. It has more than 100 member companies, including global pension funds and asset managers, listed and unlisted Asian companies, professional firms and universities.

   - Centre for International Governance Innovation (CIGI) – Michel Girard, Senior Fellow who contributes expertise in the area of standards for big data and artificial intelligence (AI).

     CIGI is a think tank that addresses significant global issues at the intersection of technology and international governance.

   - World Economic Forum (WEF). Kay Firth-Butterfield, Head of Artificial Intelligence (AI) & Machine Learning and Member of the Executive Committee.

     WEF is committed to helping ensure that AI and machine learning systems emphasize privacy and accountability, and foster equality and inclusion. The mission of WEF is to engage political, business, cultural and other leaders of society to shape global, regional and industry agendas.

   Investor (PAIB):

[230] To allow for a frank dialogue, outreach participants were informed that none of their comments would be specifically attributed to them or their organizations, but rather would be aggregated with the sum of the Working Group's outreach and evaluation thereof.

- HRL Morrison & Co – Mark Goodrick, Head of Finance and Operations, and Chris Redpath, Group Financial Controller.

  HRL Morrison is an asset manager with total funds under management of over US$ 14 billion, focusing primarily on infrastructure, private equity and property investments.

Public Sector, Oversight and Regulator Bodies (Technologist and PAIBs)

- US Government Accountability Office (US GAO) – Taka Ariga, Chief Data Scientist who leads the US GAO's Innovation Lab.

  The Innovation Lab uses novel advanced analytics and emerging technologies to drive problem-centric experiments across US GAO audit and operational teams.

- Treasury Board of Canada Secretariat and the Immigration and Refugee Board of Canada, Monia Lahaie, Assistant Comptroller General of the Treasury Board of Canada and Roger Ermuth, Executive Director and CFO of the Immigration and Refugee Board of Canada (Former Assistant Comptroller General of the Treasury Board of Canada).

  The Treasury Board of Canada Secretariat provides advice and makes recommendations to the Treasury Board committee of ministers on how the government spends money on programs and services, how it regulates and how it is managed.

- National Audit Office (NAO) of Tanzania - Sandra Chongo, Senior Auditor and Blockchain trainer.

  The NAO is responsible for auditing central government departments, government agencies and non-departmental public bodies. The NAO also carries out value for money (VFM) audits into the administration of public policy.

- Committee of European Auditing Oversight Bodies (CEAOB) – International Auditing Standards Subgroup.

  The purpose of the sub-group is to further enhance cooperation and consistency in audit oversight in the European Union regarding the adoption and use of standards on professional ethics, internal quality control of audit firms and auditing and to contribute to technical examination of international auditing standards, including the processes for their elaboration, with a view to their adoption. Members consist of representatives (from their respective Audit Oversight Board) of the CEAOB members states.

- US Office of the Comptroller of the Currency (OCC) – Robert J. De Tullio, Senior Policy Accountant and former IESBA CAG representative for Basel Committee on Banking Supervision, and Mary Katherine Kearney, Professional Accounting Fellow.

  The OCC is an independent bureau of the U.S. Department of the Treasury. The OCC charters, regulates, and supervises all national banks, federal savings associations, and federal branches and agencies of foreign banks.

- CPA Canada Public Trust Committee (PTC) and Independence Standing Committee (ISC) – Michelle Thomas, Director of Regulatory Affairs and Independence Standards, and Matt Bootle, Independence Standing Committee Chair.

  The PTC oversees the ethics standards and self-regulatory processes of the CPA Canada

profession. The ISC assists the PTC by recommending high-quality independence standards for proposed adoption by the provincial bodies in their own codes of ethics for use by all Canadian CPAs.

Technology Companies (Technologists and PAIBs)

- Savannah – Noah Baalessanvu, Head of Technology.

  Savannah is a digital transformation company in Uganda providing technology solutions and advisory services towards Africa's growth and transformation. It leverages innovation, emerging technologies and modern management practices to enable digital transformation in businesses, governments and development organizations.

- Verracy – Mary Breslin, Managing Partner and experienced fraud examiner through the extensive use of data analytics.

  Verracy provides consulting and training services to organizations around risk management, internal audit, data analytics, ethics and compliance.

- ActiveState – Jacqueline Winter, CFO, including overseeing financial reporting, HR recruiting, IT and information security, and administration.

  ActiveState provides a secure software supply chain platform adopted by 97% of Fortune 1000 companies to manage the secure implementation of open-source software.

- MindBridge AI – Danielle Cheek, VP Strategy and Industry Relations; Member, IFAC Small and Medium Practices Advisory Group; former Chair, AICPA Technical Issues Committee.

- Consensys - Professor Monica Singer, South Africa Lead at and Board member of the Accounting Blockchain Coalition (ABC).[231]

  Consensys is a blockchain technology company that builds Ethereum blockchain infrastructure and applications, and enables developers, enterprises, and people worldwide to build next-generation applications, launch modern financial infrastructure, and access the decentralized web.

- Representatives of the Institute of Electrical and Electronics Engineers (IEEE).

  IEEE has over 409,000 members in more than 160 countries, more than 60 percent of whom are from outside the United States. Members are engineers, scientists, and allied professionals whose technical interests are rooted in electrical and computer sciences, engineering, and related disciplines. IEEE and its members develop publications and

[231] ABC is led by a Board of Directors comprised of representatives from Industry leaders in the accounting, law, tax, technology and higher education. It is dedicated to educating businesses and organizations on accounting matters relevant to digital assets and distributed ledger technology, including blockchain.

technology standards dedicated to advancing technology for the benefit of humanity, as well as hold conferences and professional and educational activities.

Professional Accounting Firms (Technologist and PAPPs including consultants in advisory services, and partners within audit and assurance services as well as independence and IT risk functions):

- Deloitte AI Institute[232] – Beena Ammanath, Executive Director and Author of *Trustworthy AI: A Business Guide for Navigating Trust and Ethics in AI*.
- Ernst & Young (Global and Middle East) – Alan Young, EY Global Assurance Leader and EY Helix and Global Emerging Technology Standards Leader; Clinton Firth, Partner, Global Cybersecurity Lead for Energy and Africa, India & Middle East (AIM) Cybersecurity Leader
- KPMG (Global and Canada) – Erik Niemi, Partner, Risk Consulting Services and Global IT Attestation Services Leader; Eric Rae, Partner, Technology Risk Consulting; Renzo Francescutti, Global Independence Group Partner In Charge; Elena Zubarevsky, Managing Director
- PwC China – William Gee, Partner, Member of PwC China's Chief Digital Office
- Representatives of IFAC's Small-medium practices Advisory Group (SMP AG)

Academia:

- Representatives of the IFAC's International Panel on Accountancy Education (IPAE).

PAOs and NSSs

- Institute of Management Accountants – Loreal Jiles, Director of Research, Digital Technology & Finance Transformation, Former robotics process automation owner at bp, an energy company.
- Interamerican Accounting Association – Yvonne Huertas, President of the Technology Commission
- Representatives of Accountancy Europe – Technet
- Representatives of the IESBA-National Standard Setters Liaison Group[233]

Technology and Ethics Workshop (Middle East)

- Regional Middle East Virtual Workshop hosted by the Saudi Organization for CPAs (SOCPA)

  Participants included a mix of stakeholder attendees such as audit committee members,

[232] The Deloitte AI Institute seeks to help organizations transform with AI through cutting-edge research and innovation by bringing together the brightest minds in AI to advance human-machine collaboration.

[233] The IESBA-NSS liaison Group comprises organizations with direct responsibility for promulgating ethics (including independence) standards in Australia, Canada, China, France, Germany, Hong Kong SAR, India, Japan, the Netherlands, New Zealand, the Russian Federation, South Africa, the UK, and the US.

regulators, lawyers, academics, and technologists.

Presentations from External Parties

2. The Working Group received a number of presentations[234] on AI, RPA, Blockchain and Cybersecurity, and engaged in questions and answers (Q&A) sessions from external presenters about specific emerging technology issues to help further inform its understanding and thinking on the ethical implications of technology developments on PAs. A comprehensive playlist of the technology presentations is available on the IESBA's Technology Focus Webpage.

3. Such presentations are listed below, in no particular order:

Artificial Intelligence (Sustainability)

- *Ethics for Sustainable Artificial Intelligence Adoption: Connecting AI and ESG*[235] from Mr. Narayanan Vaidyanathan, Head of Business Insights, Association of Chartered Certified Accountants (ACCA)

Automation (Robotics)

- *Robotic Process Automation (RPA): Transforming the Finance Function* from Loreal Jiles, Vice President of Research and Thought Leadership at the Institute of Management Accountants (IMA).

Blockchain

- *Use of Blockchain in Corporate and Financial Reporting, and Regulatory Implications* from Dr. Kathleen Bakarich and Dr. John Castonguay, Assistant Professors of Accounting, Taxation, and Legal Studies in Business at Hofstra University.
- *Blockchain and Internal Control*[236] *– Relevant Insights and Perspectives* from Dr. Sri Ramamoorti, Associate Professor, University of Dayton, and Mr. Eric E. Cohen, Owner of Cohen Computer Consulting.
- *Blockchain and the Accounting Profession: Perspectives from Literature*[237] *with an Emphasis on Ethics* from Dr. Thomas Calderon, the University of Akron.

Cybersecurity

- *Cybersecurity: State of Play* from Clinton Firth, EY Global Cybersecurity Energy Industry Leader.

---

234 The Webpage provides resources to assist stakeholders follow and monitor the work of the TWG. It also provides links to ethics-related guidance and resources that are relevant to navigating the challenges and opportunities arising from evolving technologies.

235 This presentation was based on a report issued by the ACCA and Chartered Accountants Australia and New Zealand which was informed by (1) a global survey with 5,723 respondents; (2) Online discussion group with 42 professionals; and (3) expert interviews with various stakeholder industries, for example, IBM.

236 Highlighting key aspects of an August 2020 paper titled, Blockchain and Internal Control: The COSO Perspective that was commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

237 Dr. Calderon performed a summary of academic research on the topics of blockchain and presented the key observations and findings to the Working Group.

- *Cybersecurity and the Accounting Profession: A Discussion Of Ethical Implications* from Dr. Thomas Calderon, Professor of Accounting at the University of Akron.

Panel Discussions

4. As part of fact-finding, Working Group representatives also participated in various panel discussions to further diversify the perspectives gleaned relating to emerging ethics and technology or technology-related issues. Such panels discussed the following topics with other panelists:

   - *Blockchain, Smart Contracts and Related Technologies: Perspectives on Ethics*

     As part of the American Accounting Association Ethics Symposium 2021

   - *Ethics for Sustainable AI Adoption: Connecting AI and ESG*

     Hosted by the Association of Chartered Certified Accountants (ACCA) and Chartered Accountants Australia and New Zealand (CA ANZ) on Global Ethics Day 2021.

   - *Disruptive Technology and Fraud, Assurance Engagements, International Code of Ethics and Academic Research*

     As part of the International Association of Accounting Education and Research (IAAER), Taiwan Accounting Association (TAA), and National Taipei University (NTPU) Joint Conference 2021.

   - *Reimagining the profession. Are public sector organizations ready for the digital transformation?*

     As part of the CPA Canada's Public Sector Conference in 2021.

   - *Who Can Investors Trust to Provide Data Integrity and Intelligence? What Role Should Chartered Accountants Play in Tackling the Misinformation Crisis?*

     As part of the Chartered Accountants Worldwide Network USA (CAW USA) and Chartered Accountants Australia and New Zealand (CA ANZ) Beyond Accounting webinar.

Emerging Technologies Conference

5. Representatives of the Working Group attended the MIT EmTech Virtual Conference 2021 on emerging technology and global trends to help further inform its understanding and thinking on the potential ethics implications of technology developments on PAs. In particular, emerging uses of disruptive technologies on the horizon as well as how current innovative technologies are being used was presented by speakers including from IBM, Google Brain, Cisco, Microsoft, CoinDesk, Ethereum, JP Morgan Chase, McKinsey Technology, the Federal Reserve System, Allen Institute for AI; among others.

One-page Summary Table

Phase 2 Fact-finding Informed By:	PAO/NSS	Technologists	PAIBs	Firms	Oversight	TCWG	Investors	Academia	Region
Targeted Outreach									
Global Network of Director Institutes						x			Global
Institute of Corporate Directors, Canada						x			North America
Mindbridge AI		x	x			x			North America
Asian Corporate Governance Association						x			Asia
Centre for International Governance Innovation						x			Global
World Economic Forum		x				x			Global
HRL Morrison & Co							x		Asia
US Government Accountability Office		x			x				North America
Treasury Board of Canada					x				North America
National Audit Office of Tanzania		x			x				Africa
Committee of European Auditing Oversight Bodies					x				Europe
US Office of the Comptroller of the Currency					x				North America
CPA Canada Public Trust Committee	x				x				North America
Savannah		x							Africa
Verracy		x	x						North America
ActiveState		x	x						North America
Consensys		x	x						Africa
Institute of Electrical and Electronics Engineers (IEEE)		x						x	Global
Deloitte AI Institute		x		x					North America
EY		x		x					Global
KPMG		x		x					Global
PwC		x		x					Global
IFAC's Small-medium practices Advisory Group				x					Global
IFAC's International Panel on Accountancy Education								x	Global
Institute of Management Accountants	x								Global
Interamerican Accounting Association	x								South America
Accountancy Europe – Technet	x								Europe
IESBA-National Standard Setters Liaison Group	x				x				Global
Technology and Ethics Workshop hosted by Saudi Organization of CPAs	x	x	x	x	x	x	x	x	Middle East
Presentations from External Parties									
Association of Chartered Certified Accountants	x								Europe
Institute of Management Accountants	x								Europe
Hofstra University								x	North America
University of Dayton								x	North America
Cohen Computer Consulting		x							North America
University of Akron								x	North America
EY		x		x					Global
Panel Discussions									
American Accounting Association								x	North America
Association of Chartered Certified Accountants	x								Global
Chartered Accountants Australia and New Zealand	x								Asia
International Association of Accounting Education and Research								x	Global
Taiwan Accounting Association								x	Asia
National Taipei University								x	Asia
CPA Canada	x								North America
Chartered Accountants Worldwide Network USA	x								North America
Emerging Technologies Conference									
MIT EmTech Virtual Conference		x			x	x	x	x	Global

APPENDIX II: SUGGESTED NON-AUTHORITATIVE RESOURCES AND MATERIALS

1. Stakeholders highlighted many technology-related topics that would benefit from additional non-authoritative guidance to draw out potential ethics issues that might arise and how the Code applies. IFAC's IPAE, SMP AG, PAIB Committee and other PAOs are encouraged to develop such material. Key topics include:

Topic	**Detail**
Ethical Leadership and the Code's Fundamental Principles	Against the context of the Code's requirement for a PA to act in the public interest, highlight the expectations for a PA relating to technology, and its design, development, implementation or use.
AI Ethics Frameworks and the Code's fundamental principles	Illustrate how the Code's fundamental principles compare to the common themes in over 190 AI Ethics Frameworks issued by various organizations, for example, the UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (November 2021).
Managing Bias in Technology and Data	Demonstrate how the Code's fundamental principles and conceptual framework applies to identify and mitigate the effect of bias, and in particular, the risk of unconscious automation bias, when using technology and data.
Maintaining Objectivity when Relying on Technology Experts	The extent that a PA can rely on technology experts, and how to ensure sufficient oversight
Threshold of Competence	Characterize what is a sufficient threshold of competence in the context of the Code and the IESs and illustrate what it means to understand, and hence explain technology, its inputs and outputs.
Level of Audit Documentation:	The extent of documentation needed when using, for example, AI or Blockchain smart contracts
Data governance, including privacy and security	Highlight PAIB and PAPP expectations with respect to data collected, stored, held, secured, protected and used. Also consider highlighting PA expectations regarding data governance over: (a) data collection including quality of metadata management, (b) data access and controls, and (c) objectivity in data analytics The evolving laws and regulations on AI and data privacy are forming a patchwork of different laws and regulations, both cross- and intra-jurisdictional, which creates uncertainty. Documenting consistent minimum expectations for PAs to comply with their ethics obligations is valuable.

Topic	Detail
	Outlining the risks that arise from third party access (i.e., third party service providers) and cybersecurity issues.

2. Finally, stakeholders emphasized that "asking the right questions" to challenge assumptions, inputs and outputs of technology is key, and that it would be helpful to share such best practices and expertise across PAOs either through a forum or platform of sorts. In this regard, stakeholders also noted that developing non-authoritative guidance that draw parallels to real use-cases or scenarios to illustrate the application of Code is a format that is very helpful to PAs.