Agenda Item 9-A

Technology—
Issues and Task Force Preliminary Views

I. PURPOSE OF THIS PAPER

1. This paper provides a summary of the Task Force's preliminary views on how to pursue two of the recommendations outlined in the approved IESBA project proposal, *Enhancing the Code in an Evolving Digital Age*.

2. The IESBA is asked to provide input on the following:

Matters for IESBA Consideration

1. IESBA members are asked to provide directional input on the following:

   (a) With respect to Recommendation 2, the Task Force identified four options to address threats to the Fundamental Principles created by the complexity of the professional environment in which professional accountants (PAs) perform their professional activities. In this regard, the Board is specifically invited to comment on each of these options (see paragraph 20) and provide directional input.

   (b) With respect to Recommendation 7, the Task Force considered numerous use cases where technologies are being deployed by firms with their clients, including the sale or licensing of new tools and new types of non-assurance service engagements. The Board is specifically invited to comment on the Task Force's preliminary views presented in paragraph 49, as well as on the illustrative diagram included as Appendix B.

   (c) The Task Force prioritized the other recommendations and will progress through them in due course (see paragraph 56). The Board is asked for any high-level thoughts on prioritization of the remaining recommendations and next steps, including any further research that the Board believes would be helpful.

II. BACKGROUND

3. The objective of the project is to enhance the Code's provisions in response to the transformative effects of major trends and developments in technology in order to maintain the Code's robustness and relevance as a cornerstone of public trust in the global accountancy profession.

4. The IESBA committed in its Strategy and Work Plan, 2019-2023 to a major strategic initiative on Technology. Through this initiative, the IESBA aims to gather an understanding of the transformative effects of trends and developments in technology on the assurance, accounting and finance functions, and explore their ethical implications for the *International Code of Ethics for Professional Accountants (including International Independence Standards)* (the Code).

5. In December 2018, the IESBA established a Working Group[1] with a mandate to:

   (a) Identify potential ethical implications of technology developments on the robustness and relevance of the fundamental principles and independence standards, in terms of both challenges to PAs' compliance with requirements under the Code and ways in which technologies could be used to support and enhance compliance;

   (b) Develop proposed responses to address any identified ethical implications, whether through revisions to the Code or through developing non-authoritative material; and

   (c) Identify specific outreach and partnership opportunities to share knowledge and to promote the Code as an effective tool for PAs to refer to in addressing ethics issues related to the use and effects of technology on their professional activities.

6. In pursuing its objectives, the IESBA took a phased approach to the technology initiative. Phase 1 focused on the two areas of (a) artificial intelligence (AI) and robotic process automation (RPA), and (b) Big data and data analytics. This focus reflected the fact that these technological developments are currently the most pervasive and affect the broadest population of PAs.

7. Following fact finding, including a substantial program of outreach to stakeholders, the Working Group delivered its report of findings and recommendations to the IESBA in December 2019 (Phase 1 Final Report). At the March 2020 meeting, the IESBA approved a project proposal to develop enhancements to the Code based on the findings and recommendations in the Phase 1 Final Report and established the Technology Task Force.

8. The Task Force has commenced its work to pursue the seven recommendations for enhancements to the Code as set out in the approved project proposal.

9. From the Task Force's initial review of the recommendations in the project proposal, the Task Force prioritized two recommendations:

   - Recommendation 2, under the heading of *Complexity of the Professional Environment,* was prioritized, recognizing that this recommendation would benefit from more time for consideration and deliberation by the Board and might impact the other recommendations. There is also an opportunity to collaborate with the Tax Planning Working Group, as one of that group's preliminary findings included the impact of complexity on PA decision-making and its posing of new challenges.

   - Recommendation 7, under the heading of *Independence,* was prioritized given the extent of overlap with the Non-assurance services (NAS) Task Force deliberations and the more immediate practical questions arising from stakeholders.

10. This paper outlines the Task Force's preliminary views on these two recommendations. The paper is structured as follows:

[1] In view of the interoperability of the Code with the standards of the International Auditing and Assurance Standards Board (IAASB) and the strategic priority given by both Boards to addressing the developments in technology, the IESBA agreed to coordinate its work in this area with the IAASB. As a result, the IESBA's Technology Task Force is linked to the IAASB's Technology Working Group through the participation of a correspondent member from each Board on the other Board's Task Force/Working Group.

Preliminary Observations: Complexity (Recommendation 2)

- How does "complexity" manifest for PAs and what impact does this have?
- Why focus on complexity now?
- Elements of "complexity"
- To what extent is complexity missing from the Conceptual Framework?
- Options to address complexity

Preliminary observations: Independence (Recommendation 7)

- New technology-enabled tools and related types of NAS engagements
- Where do these new tools and service engagements fit within the Code?
- Additional thoughts on drafting geography
- Preliminary view

III. TASK FORCE PRELIMINARY OBSERVATIONS: COMPLEXITY (RECOMMENDATION 2)

How does "complexity" manifest for PAs and what impact does this have?

11. The Task Force identified a number of examples of complexity that PAs face as a result of technology developments or how technology is being used in an increasingly complex world and the impacts that these uses are having:

- Developing and working with disruptive technology is not necessarily a core competence of a PA; however, PAs are increasingly taking on responsibility in developing and using such technology in order to meet employer, client, and market expectations and needs. Taking on such increased responsibility with insufficient professional capacity threatens PAs' compliance with the Fundamental Principles of Professional Competence and Due Care, as well as Integrity, Objectivity and Professional Behavior.
- Some AI applications and underlying algorithms have become or are becoming autonomous and deep learning allows them to adapt without it being easy or even possible for humans to fully understand the adaptations taking place.
- Rapid but constant change in standards, regulation, and legislation, including technology-related legislation such as data privacy acts, creates significant compliance challenges, particularly for PAs exposed to such change across a broad range of different jurisdictions and professional activities.
- Despite the pace of standards, regulatory, and legislative change, this continues to be outpaced by the exponential rate of change in the development and use of many disruptive technologies. Such standards and regulatory lag results in PAs needing to operate in periods of increased uncertainty and increased reliance on principles-based approaches (for example, the emergence of cryptocurrencies and the lag time as to how to regulate and account for such activity).

Why focus on complexity now?

12. Dealing with some level of complexity is clearly not new for PAs. For example, the perception of "standards overload" has been observed for many years. The Task Force's focus is on the factors that have changed (or are changing) that bring complexity further to the fore, especially as a result of technological developments. This focus is based directly on the input of numerous stakeholders as documented in the Phase 1 Final Report.

13. The Task Force recognizes that although various technologies have an exponential impact on complexity, technology is not the only driver. As a result, the Task Force looked to encapsulate complexity more broadly, identifying complexity drivers in various forms, for example:

    - A lack of congruence or conflicting tax rules resulting in transfer-pricing regimes and interjurisdictional tax planning becoming so complex that they result in uncertainty and might overwhelm the PA.
    - Black-swan events – for example, the COVID-19 pandemic, global financial crises, and other national and regional crises (including natural disasters) – that starkly illustrate how complexity can be particularly daunting and magnified during such events and periods where the consequences of the outcome are significant (e.g., lack of preparedness; lack of buffers; urgency and intensity; human impacts of stress; concentration of issues; high uncertainty; interdependencies that are more notable when businesses and/or lives are on the line).
    - Globalization and increased interdependency between organizations and professions, as well as radically changing business models.
    - Broader range of possible accounting or measurement estimates resulting from complicated, interconnected uncertainty.
    - New areas of measurement, decision-making, reporting and assurance on such reporting (e.g., sustainability reporting, climate change, etc.).
    - Increasing breadth of firm practice areas.
    - Disruptive effects that some new technologies are having on professional activities and on the profession in general (especially as professional accountancy organizations address questions around the relevance of the PA role to meet changing expectations).
    - Both widening and deepening competence expectations to meet changing needs of employers, clients, and other organizations and stakeholders.

Elements of "complexity"

14. The Task Force identified the following elements that are commonly inherent in circumstances where complexity is present:

    (a) Exponential pace of change

    (b) Lack of transparency/explainability in technology being adopted

    (c) Uncertainty/ambiguity/contradictory forces, regulations/legislation, and guidance

    (d) Overwhelming nature and level of intensity

    (e) Resource constraints, including intensified time pressure ("do more with less")

(f) Capability constraints, including both ability and capacity to perform competently (e.g., unfamiliarity).

To what extent is complexity missing from the Conceptual Framework?

15. The Task Force considered whether the Code already leads a PA to specifically consider the impact of complexity, either related to technology or more broadly, on compliance with the FPs to identify whether a gap in the Code is coming to light as the business environment and technology (often interrelated) have become materially more complex.

16. In many instances, the identified elements of complexity highlight ever increasing pressure being placed on a PA. As noted in the Role and Mindset ED, part of the scope of that project was to address threats to compliance with the fundamental principles arising from bias and pressure. The IESBA considered adding application material on bias in the Code to highlight that bias is a potential threat to compliance with each of the fundamental principles. However, given the significance of bias, the IESBA determined that it would be more appropriate to include new text in Section 120.

17. The Task Force considered whether it was necessary to explicitly address threats to compliance with each of the fundamental principles from complexity and all its elements, including the element of pressure. Based on its deliberations to date, the Task Force reached the preliminary view that the Code does not adequately address the impact of "complexity." Within the existing threat categories laid out in paragraph 120.6 A3, there is no clean fit or clear trigger to prompt a PA to consider how complexity and its multiple facets might threaten their compliance with the Fundamental Principles. The Task Force considers this to be a risk. If a PA cannot easily identify their situation as falling into one or more of the listed threat categories, they might incorrectly assume that an otherwise valid threat does not need to be evaluated and, if necessary, addressed.

18. Appendix A includes examples identified where there is no obvious link to prompt a PA to identify the threats described in paragraph 120.6 A3 of the Code that might be created by complexity. These examples nonetheless lead to potential threats to compliance with the Fundamental Principles of Integrity, Objectivity, Professional Competence and Due Care, and Professional Behavior.

19. The Task Force is of the view that there is significant value in signaling to PAs a need to reflect on the impact of increasing complexity on compliance with the Fundamental Principles, for example, to identify threats in situations that are overwhelming or where unrealistic expectations to be an expert in all things threaten compliance with one or more of the Fundamental Principles or with Independence.

Options to address complexity

20. The Task Force has identified four, non-mutually exclusive, options to resolve the identified gaps:

Option 1	Modify those paragraphs in Section 120[2] that reference the existing five threat categories to permit additional threat categories to exist, whether explicitly listed in the Code or not

[2] For example, paragraphs 120.6 A2-A3 and 120.12 A2

Option 2	Amending the existing five threat categories, as appropriate, in paragraph 120.6 A3 to build in missing elements of complexity
Option 3	Add one or more threat categories to paragraph 120.6 A3
Option 4	Highlight complexity in a manner similar to the approach taken by the Role & Mindset Task Force with respect to bias

21. The Task Force sees merit in all of these options.

OPTION 1:

22. The Task Force recommends pursuing Option 1 given the following:

- The Code states that "Threats to compliance with the fundamental principles might be created by a broad range of facts and circumstances. It is not possible to define every situation that creates threats. In addition, the nature of engagements and work assignments might differ and, consequently, different types of threats might be created."[3] Given this, it appears internally inconsistent to pre-suppose that all threats to compliance with the Fundamental Principles may be categorized into one of five threat categories.
- There are a number of threats that do not readily fit into the existing categories, such as the various elements of complexity and resulting pressures, over-reliance on technology due to lack of explainability, inherent biases, etc. Not all of these are new, of course; however, many of them were identified by the Technology Working Group to exist in a disruptive technology context through both desk research and direct discussions with stakeholders.
- Opening up the threat categories beyond those specifically identified in the Code better aligns with PAs' actual experience when assessing a situation to identify potential threats to compliance with one or more fundamental principles. Allowing for threats that do not fall into the existing five categories also better supports a principles-based Code, particularly as such threats might arise from an unlimited number of possible behaviors and contexts. Although providing some pre-defined, more common categories offers a helpful starting point as guidance, they are not definitive when identifying threats and ought not to constrain a PA from evaluating and addressing a threat that they have identified just because it is not on the pre-defined list.
- The Task Force reflected on possible concerns that opening up the threat categories in paragraph 120.6 A3 might make it more difficult to assert compliance with the Code. However, this concern was dismissed as the paragraph is application material and not a requirement (i.e., it assists the PA in applying the requirements, rather than being prescriptive in nature).
- Opening the lead-in paragraph 120.6 A3 to allow for still other threat categories based on a PA's own assessment and description will future-proof the Code and is more principles-based. The Conceptual Framework specifies an approach to identifying threats to compliance with the Fundamental Principles and to Independence, and then evaluating and addressing the threats identified. Whereas application material is useful to assist in this process, it should not require

[3] Paragraph 120.6 A2

a PA to have to artificially "shoe-horn" their specific experience into existing categories in order to apply the Conceptual Framework. Tweaking the wording of existing threat categories and adding new ones might well benefit users, but will almost certainly still not present a complete picture.

- There is some precedent in other organizations that take a more open approach to identifying threats as well, for example:
    - The AICPA Code[4] has seven threat categories and acknowledges that there might be more.
    - CPA Canada only applies the pre-defined five threat categories to compliance with the Independence standards. No specific categories are defined for the remainder of the CPA Canada Code.
    - The International Valuation Standards Council has six threat categories, including a "client conflict threat" (the threat that two or more clients may have opposing or conflicting interests in the outcome of a valuation, which would not neatly fit into our Code's five threat categories).
    - The Chartered Body Alliance (a joint initiative by the Chartered Insurance Institute, Chartered Institute for Securities & Investment and the Chartered Banker Institute) is developing a Code of Ethics which does not describe specific threats.
- An important PA competence involves exercising professional judgment. Acknowledging the potential for threats that do not fall into any of the five categories, such as the large variation of different elements of a complexity threat identified above, supports and encourages PAs to use their professional judgment in an ethics context to determine whether there are additional threats to compliance with the Fundamental Principles and Independence that they need to evaluate and address.

23. An example of how Option 1 might be reflected in the Code would be to amend the following paragraphs to permit additional threats to exist, even without explicitly listing new categories in the Code. The mark-up from the extant wording below is only meant to reflect an indicative approach to implementing Option 1:

    120.6 A3 Many ~~T~~threats to compliance with the fundamental principles fall into one or more of the following categories: […]

    120.12 A2 […] ~~The categories of~~ Many threats to compliance with the independence requirements fall within one or more of the categories ~~the fundamental principles~~ described in paragraph 120.6 A3 ~~are also the categories of threats to compliance with independence requirements~~.

24. The Task Force recognizes that Option 1 on its own is unlikely to be sufficient as it does not draw out the elements of complexity identified and therefore recommends that Option 1 be considered in conjunction with one or more of the other options.

[4] See AICPA Code of Conduct 1.000.010.08-.16, which begins: "*Many threats* fall into one or more of the following seven broad categories: adverse interest, advocacy, […]"

OPTION 2:

25. From the Task Force's initial review of the five threat categories in paragraph 120.6 A3, the closest ties for the elements of complexity were made to the self-interest and intimidation threats, although arguably neither the descriptions nor the common application of these threat categories intuitively lands one to classify "complexity-related" situations in this way. For example:

    - Self-interest:
        - Wanting to protect one's job by not admitting to being overwhelmed or simply not having the capacity to understand or fully recognize the issue at hand.
        - Not being able or willing to commit, or not prioritizing, the time and other resources to develop additional competence or seek out others with the required competence.
    - Intimidation:
        - Feeling pressure that the PA needs to be an all-around business expert, such as being conversant with a particular technology.
        - Pressure of being overwhelmed and incapable or not having the capacity or support to take on a new responsibility.

26. For Option 2, the Task Force identified possible ways to incorporate some of these complexity elements within the existing five threat categories to address gaps through broadening the existing threat categories and recognizing the impact of technology and the elements of complexity more directly. An indicative approach, reflecting mark-ups from the extant wording, of how this option might be reflected in one of the current threat categories (intimidation threat) follows:

    120.6 A3(e) ~~Intimidation~~ Pressure threat - the threat that a professional accountant will be deterred from acting ~~objectively~~ appropriately because of actual or perceived constraints, expectations, or intimidation ~~attempts to exercise undue influence over the accountant.~~

27. Broadening the title explicitly messages a greater range of pressures in this category than simply "intimidation"[5] and more easily enables relevant examples being included at appropriate locations in the Code. Changing the title also recognizes that intimidation is *one* form of pressure, but that there are other pressures that might threaten compliance with the fundamental principles. Arguably in any case, "intimidation" goes beyond identifying a threat and pre-determines an unacceptable level of threat.

28. The benefit of amending the existing threat categories would be to explicitly prompt a PA to identify how the pressure elements related to complexity may threaten compliance with the fundamental principles.

29. The Task Force is, however, cognizant of potentially moving too far away from the existing threat category descriptions and thereby diluting the threat categories or confusing users who are deeply familiar with them, as the existing categories have been in use (both academically and in practice) for many years.

[5] Oxford Dictionary definition: "to frighten or threaten somebody so that they will do what you want"

OPTION 3:

30. In addition to, or as an alternative to, Option 2, the Task Force identified new threat categories that could reasonably be added to the existing five categories in paragraph 120.6 A3. Within the context of the observations noted in the Phase 1 Final Report, the Task Force identified "complexity," "over-reliance," or even "bias" as potential new threats that are related – but not limited – to technology.

31. An example of how a new complexity threat might be included in paragraph 120.6 A3:

> 120.6 A3(f) Complexity threat – the threat that a professional accountant will be unable to make an informed judgment because of complicated and interrelated facts and circumstances.

32. The benefit of capturing the missing elements in new threat categories is to avoid diluting existing concepts and create an even more explicit prompt for PAs to identify how complexity, for instance, might threaten their compliance with fundamental principles or independence.

33. Arguments against introducing one or more additional threat categories include:

- The difficulty in drafting a description that effectively incorporates the various elements currently identified as subcomponents of a "complexity" threat. If Option 1 were also adopted, this challenge would be mitigated, as the defined threat categories would not need to be exhaustive. Additionally, other relevant examples could be included in other parts of the Code.
- Complexity is pervasive. The difficulty in defining a "complexity threat" is that it may appear too "ordinary" as PAs face at least some complexity in almost all scenarios. For example, it might be onerous to require PAs to identify and evaluate all complexity threats. A contrary perspective is that this is no different from a self-interest threat in that a PA is commonly faced with interests that have the potential to inappropriately influence their behavior, but in normal circumstances these do not rise to the level of needing attention – the same is true of complexity.
- Complexity and/or over-reliance might not be threats in and of themselves, but rather factors that need to be considered within the context of applying professional judgment, similar to the Role & Mindset Task Force's implementation of the concept of bias in the Code, which led to Option 4 being considered. An opposing view is that there is an argument to include bias as a threat category to compliance with one or more fundamental principles and to independence, as several forms or manifestations of bias do not fall into the existing threat categories.

OPTION 4:

34. Option 4 would take a different approach, not linked to threats, but more broadly to the circumstances that impact on the application of the conceptual framework and/or application of professional judgment as it relates to complexity and all of its elements. Follow-on work would include adding further prompts for the PA to consider how complexity relates to each fundamental principle within Section 120. This approach might follow a similar approach to the Role & Mindset's approach to bias.

35. This option avoids the challenges identified by amending the threat categories and/or adding new categories. The risk is that this approach will not be as effective in drawing PAs' attention to the need to consider the elements of complexity as would be adding one or more new threat categories. Also, if the Board accepts that complexity, and perhaps over-reliance and bias, are genuine threat categories – and cannot logically be differentiated from the existing threat categories – then it would be more consistent to include one or more of these as guidance in paragraph 120.6 A3.

36. The IESBA is asked to provide input on the following:

> **Matter for IESBA Consideration**
>
> The Task Force identified four options to more effectively deal with the threats to compliance with the fundamental principles created by the complexity of the professional environment in which PAs perform their professional activities. In this regard, the Board is specifically invited to comment on each of these options (see paragraph 20) and provide directional guidance.

IV. TASK FORCE PRELIMINARY OBSERVATIONS: INDEPENDENCE (RECOMMENDATION 7)

New technology-enabled tools and related types of NAS engagements

37. With respect to this recommendation, Task Force discussions were given structure by looking at potential new tools and NAS engagements that are emerging and being marketed by firms and reported by regulators. Examples include, but are not limited to:

- Hosting, storing or synchronizing client data
- Data analysis or modelling, including: data mining, data visualization and data integration
- Developing intelligent agents for risk assessment or forensic services
- Developing platforms for presenting and promulgating content
- Developing blockchain-based business applications, including e-commerce
- Cybersecurity penetration testing of systems
- Using technology to test business continuity or disaster recovery provisions.

38. The Task Force intends to continue canvasing stakeholders to identify additional emerging tools and services, which will continue to inform the approach under consideration.

39. In order to categorize the evolving technology tools and non-assurance service engagements, a diagram (included as Appendix B) was developed to help assess how Section 600, and its sub-sections as currently reflected in the NAS exposure draft, might include such new tools and services. Three fundamental questions are:

i. Do these new tools, in fact, constitute (at least in part) “services,” such that they fit intuitively into the NAS provisions?

ii. Does firm-developed technology (applications, systems or tools) that is licensed to clients have a “product” element and, if so, how should this be addressed in the Code?

iii. Are there new service types emerging that would be considered NAS, but do not readily fit into the existing sub-sections within section 600?

Where do these new tools and service engagements fit within the Code?

40. The Task Force formed the preliminary view that some new technology-related engagements reflect or involve a pure service and are already covered by the subsections in Section 600. In addition, many of the new types of engagements contemplated likely already fit within the extant intent (and potentially also wording) of subsections 601 to 605 or 607 to 610:

- 601 Accounting and bookkeeping services (e.g., automated transaction processing)
- 602 Administrative services (e.g., intelligent document management or data aggregation)
- 603 Valuation services (e.g., valuations based on AI-enabled predictive models)
- 604 Tax services (e.g., AI-enabled tax minimization tools)
- 605 Internal audit services (e.g., cybersecurity penetration testing)
- 607 Litigation support services (e.g., AI-enabled prediction of success at trial)
- 608 Legal services (e.g., AI-enabled legal document scanning or predictive analytics)
- 609 Recruiting services (e.g., AI-enabled résumé screening)
- 610 Corporate finance services (e.g., blockchain-based data visualization to provide information in real-time for better decision making)

The only difference is that in many instances advanced technology is being employed to provide or augment the services traditionally offered in a less technologically enabled manner. At the extreme, the technology is (or will be) operating fairly autonomously. This is akin to the firm providing technology to replace some or all of the tasks normally performed by a PA staff member.

41. There are also situations where the firm is engaged to design or implement a system for a client. Even though the system being designed or implemented could be viewed as a "product," the firm's role is limited to designing and/or implementing the client's system, which reflects a service and hence is included within subsection 606.[6]

42. There might be other NAS engagement types that are now enabled by new technologies that do not fit within the current NAS subsections 601 to 610. In other words, disruptive technologies might have given rise to new types of services that were not possible, contemplated, or economically feasible before. For such new services, the Task Force is of the view that a new subsection would be drafted, but that it – importantly – be defined by the type or objective of the new service being offered, and not by the technology being used to perform the service (e.g., "autonomous decision support services," as opposed to "using AI or intelligent agents").

43. Another option is for a firm to develop and maintain ownership of a technology tool or application and license it to clients, either with or without client-specific customization. The Task Force's view is that this is most similar to a software product licensing arrangement for the underlying ("base") version of the tool or application and that a new form of business relationship is created. This form of business relationship could be included in Section 520[7] (particularly as there might be instances where a firm and client seek to collaborate and jointly develop a new tool or application to market to third parties, something already considered within Section 520). Any customization being performed for an individual client would be viewed as a design or implementation NAS and is thereby also captured by subsection 606. Finally, if the tool or application performs a service that is contemplated within subsections 601 through 610, then it also gives rise to the need to consider those provisions. For example, where a client inputs data into tax return preparation software developed by the firm and licensed or sold to the client, subsection 604 would be applicable.

---

6 Information Technology Systems Services

7 Section 520, *Business Relationships*

44. Any maintenance agreement related to the base version of the tool or application could be viewed as an extension of the business relationship because there is no specific engagement with any given client to perform normal updates to the tool or application. Where additional customization is required for a particular client's update, normally as a result of initial customization that was performed for that client, this would again be expected to fall under Section 606 of the Code.

Additional thoughts on drafting geography

45. The "product versus service" classification question is challenging, as Section 600 and its subsections purposefully reference non-assurance *services*.

46. Conceptually it may be useful to fully separate a product from a service**,** but this might be more difficult in practice. A number of examples highlighted that in practice there is a product-to-service continuum, with relatively few examples of a pure product or a pure service; rather, there are more examples of "products" that are a combination of products and services, as well as new products that take on the role of delivering services traditionally performed by PAs more directly (e.g., tax return preparation software that optimizes client decisions around minimizing tax).

47. The product/service distinction will have relevance outside of the Code as well, in a way that may impact interpretation and behavior. For example, the U.S. SEC's independence rules[8] prohibit business relationships between the auditor and their audit client. Such prohibited business relationships, however, specifically do not include providing professional services to the audit client. A "professional service" is not defined, and this distinction might evolve over time, raising questions as to where the sale or licensing of a firm's technology product fits.

48. The Task Force identified the following factors that might be useful to determine whether the NAS sections or an amended Section 520 apply:

    i. The output that is created, whether a person or technology is generating the output, and the extent to which the technology is replacing an activity that would otherwise be performed by a person (audit firm staff).

    ii. The need for any ongoing contractual relationship.

    iii. The extent to which the output incorporates the PA's professional competence or is balanced against a need for the client to apply their own expertise.

    iv. Variation in revenue stream may come from repackaging the same output – either "lend staff" to do task (charge per hour) or replace with the firm's technology tool that performs that task – payment up front versus payment spread? Technology may make the service more efficient and more accurate and consistent.

    v. Ownership, licensing, and/or location of the technology (e.g., firm or client owned, cloud-based or hosted on the firm's, client's, or a third party's server).

    vi. Who operates the technology (e.g., firm staff or client staff).

    vii. The extent of customization for a specific client's needs.

[8] SEC Rule 17 CFR 210.2-01(c)3

viii. The extent of the client's engagement in understanding what the technology is doing and ensuring that it meets their business needs.

ix. Any ongoing responsibility for the firm to maintain the technology over time.

x. Any joint development (by firm and client) and marketing or use of the technology tool to third parties.

Preliminary view

49. The Task Force's preliminary view is that new types of engagements and the sale or licensing of new tools can best be incorporated in the Code as follows:

- Engagements that reflect "pure" services fit within the existing subsections of section 600; adjustments to wording might be beneficial to ensure that their inclusion is apparent;
- The sale or licensing of a tool developed by a firm can be best addressed by expanding section 520 to address the potential business relationship that might result; and
- To the extent that new engagement types are emerging that are not encapsulated within extant subsections 601 to 610, new subsections should be developed based on the nature or objective of the service (and not based on the specific technology being used).

50. The IESBA is asked to provide input on the following:

Matter for IESBA Consideration

The Task Force explored various locations in the Code in which to address threats arising from new types of engagements and from the sale or licensing of new technology tools. The Board is specifically invited to comment on the Task Force's preliminary view presented in paragraph 49 as well as on the illustrative diagram included as Appendix B.

V. NEXT STEPS

51. The Task Force has identified a series of questions to explore for each recommendation and will survey key stakeholders as part of its outreach.

52. The Task Force intends to seek input from National Standard Setters (NSS) as a follow up to the May 2020 NSS meeting and key regulators in Q3 2020, and others subject to stabilization of the ongoing COVID-19 pandemic.

53. The Task Force Chair, together with IESBA senior staff, is in ongoing discussions with IFAC on developing thought leadership and other non-authoritative materials addressing the topics identified in the Phase 1 Final Report. There may be opportunities to partner with other stakeholders.

54. Work to consider the remaining recommendations from the approved project proposal is being initially advanced by individual Task Force members and will next be considered by the full Task Force or its small teams, as appropriate.

55. The Task Force anticipates presenting a further draft of any proposed amendments to address the complexity and independence matters, together with an update on the remaining recommendations and developments related to non-authoritative materials, at the September 2020 IESBA meeting.

56. Other than rating the relative priority of Recommendations 2 (Complexity) and 7 (Independence) as **Higher**, the Task Force determined relative priorities of the other recommendations as follows:

- R1 – Broader societal role of PAs when developing and using technology: **Lower**
- R3 – Transparency: **Moderate**
- R4 – Accountability: **Moderate**
- R5 – Privacy and Confidentiality: **Higher**
- R6 – Enabling Competencies and Skills: **Moderate**

57. The IESBA is asked to provide input on the following:

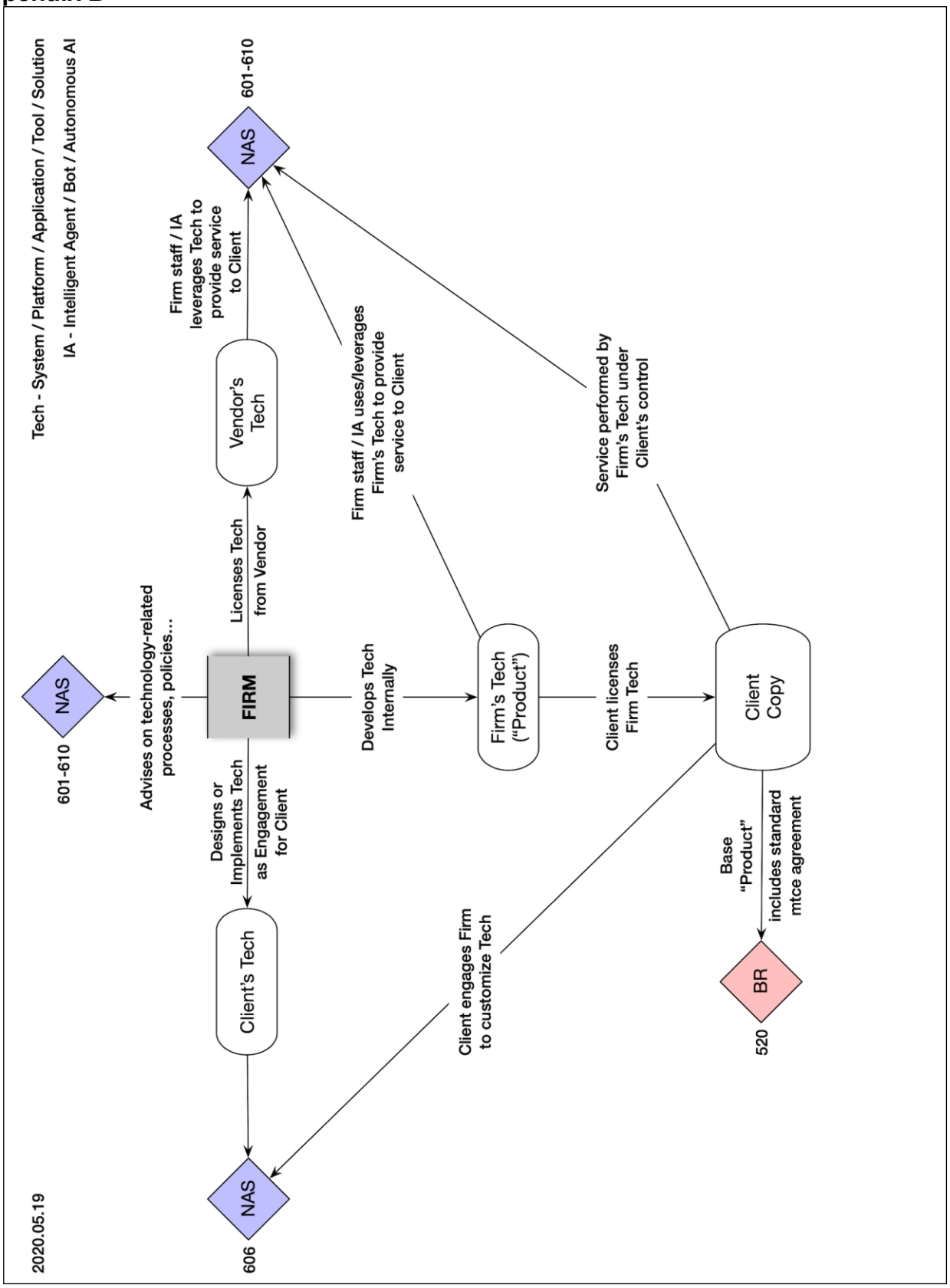
Matter for IESBA Consideration

The Board is asked for any high-level thoughts on the prioritization of remaining recommendations and next steps, including any further research that the Board considers would be helpful.

Appendix A: Potential Gaps in the Existing Threat Categories

Situation	Potential Outcome	FPs Threatened	Threat categories
A PAIB relies on an "black box" intelligent agent to determine an estimate in a high-stakes decision.	Estimate is flawed, and decision leads to significant harm to the organization and the public.	PC&DC Objectivity (over-reliance on tech) Professional behavior	"Complexity" "Over-reliance" / "Bias"
The PAPP's client uses an AI system to estimate the fair value of its intangible assets. The algorithm uses deep learning. Initially, the calculations were similar to more traditional calculations but over time the AI valuation appears to be growing at a higher rate than expected by the PAPP.	If the algorithm lacks explainability, the auditor might not be able to properly assess the extent to which evidence is sufficient and appropriate.	PC&DC	"Complexity"
A PAIB's employer operates projects in a country known for high corruption. During a crisis, the PA needs to make a decision to release funds quickly, without sufficient time to be able to understand the full implications of the situation or apply normal controls.	The funds end up being used in a public official bribery scheme.	PC&DC Integrity Professional behavior	"Complexity" "Pressure"

Appendix B


Tech - System / Platform / Application / Tool / Solution
IA - Intelligent Agent / Bot / Autonomous AI
NAS
601-610
Advises on technology-related processes, policies…
FIRM
Licenses Tech from Vendor
Vendor's Tech
Firm staff / IA leverages Tech to provide service to Client
NAS
601-610
Designs or Implements Tech as Engagement for Client
Client's Tech
NAS
606
Develops Tech Internally
Firm's Tech ("Product")
Firm staff / IA uses/leverages Firm's Tech to provide service to Client
Client licenses Firm Tech
Client Copy
Service performed by Firm's Tech under Client's control
Client engages Firm to customize Tech
Base "Product" includes standard mtce agreement
BR
520
2020.05.19