Technology – Survey results

Matters for IESBA Members' Consideration

IESBA Members are asked to provide thoughts on the key messages received in response to two technology surveys undertaken in Q4 2020.

I. BACKGROUND

1. In October 2020, the IESBA Technology Task Force launched two online surveys seeking stakeholder feedback to inform its consideration of issues related to two key recommendations in the February 2020 Phase 1 report of its Technology work stream, *Technology Working Group Phase 1 Final Report*. The topics addressed by these surveys were:

   i. Technology and complexity in the professional environment; and

   ii. The impact of technology on auditor independence.

2. Responses were sought by November 25, 2020 (extended from November 10, 2020).

3. This document summarizes key themes and insights from the survey results. The views expressed herein are not views of the Technology Task Force, but rather views that were expressed in the survey responses. The Technology Task Force has not reached any conclusions regarding the matters below but will use this feedback to inform possible future actions on the topic of technology and the impact on the *International Code of Ethics for Professional Accountants (including International Independence Standards)* (the Code).

II. TECHNOLOGY AND COMPLEXITY IN THE PROFESSIONAL ENVIRONMENT

Overview of Respondents

4. 108 responses were received, including from 41 practitioners, 32 professional accountancy organizations (PAOs),[1] 11 academia, 7 national standard setters (NSS), 4 government/public sector 3 investors, 3 regulators,[2] 3 Those Charged with Governance, 2 corporate and 2 other.

5. Geographically, responses were spread across North America (22); Asia-Pacific (20); Africa (20); Europe (18); the United Kingdom (15); South America (9); Middle East (2) and unidentified (2).

6. In the summary of key themes presented below, in most instances, views were supported by a mixture of stakeholder groups from a range of jurisdictions.

Elements and Examples of Complexity

7. In its previous IESBA June agenda paper, the Task Force had identified the following elements that are common in circumstances where complexity is present. Respondents to the survey supported such elements:

[1] One respondent provided feedback via a teleconference rather than via the survey template

[2] One respondent provided feedback via a teleconference rather than via the survey template

Non-mutually exclusive elements	# respondents	Percentage
Exponential pace of change	73	68%
Resource constraints, including intensified time pressure ("do more with less")	72	67%
Capability constraints, including both ability and capacity to perform competently (e.g., unfamiliarity)	59	55%
Lack of transparency/ explainability in technology being adopted	57	53%
Overwhelming nature and level of intensity	45	42%
Uncertainty/ ambiguity/ contradictory forces	36	33%

8. In response to an open-ended question on examples of complexity experienced in a Professional Accountant's (PA) professional environment, respondents generally cited the following (often in the context of an audit):

   - Technology transformation, including amongst others: Artificial Intelligence and Machine Learning, Data Analytics, Robotic Process Automation, Optical Character Recognition, Drone and satellite usage, Blockchain-based solutions, and cloud computing, Internet of Things (IoT).
   - Cyber-security and privacy issues exacerbated by remote working, heightening fraud/corruption.
   - Company culture, including a lack of "appropriate" tone from the top or attitude.
   - Laws, regulations and professional standards (including tax legislation, International Standards on Auditing (ISAs), the Code and other professional standards) not being plain language and cross border implications of various national or jurisdictional laws.
   - Valuations, going concern estimates and expected credit loss models, which are exacerbated with uncertainty arising from the COVID-19 pandemic.

Threats that are Not Captured in the Code

9. Survey respondents were asked if there are any threats to the Fundamental Principles which are not appropriately captured within the existing five categories of threats in the Code:

	"Yes"	"No"
% respondents	26%	74%

10. No reasons were provided by respondents that selected "No". Respondents generally provided the following reasons for selecting "Yes":

    - Being unaware of bias embedded in the autonomous software algorithms.

- A lack of transparency and explainability of some technologies.
- An inability or unfamiliarity of the PA to understand algorithms.

11. In addition, a few respondents noted that:

- The current definition of self-review threat in paragraph 120.6 A3 of the extant Code does not allow for activities or judgments performed by technology.
- Technology is enhancing the connectivity between the client and the professional service provider, which blurs the boundary between employee responsibilities and professional engagement and impairs decision making.

Options to Address Complexity in the Code

12. In its previous IESBA agenda papers in June and September 2020, the Task Force had observed that within the existing threat categories in the Code, it appears that 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.[3] Four non-mutually exclusive options were explored as possible ways to incorporate complexity and its elements into the conceptual framework:

Option 1	Modify paragraphs 120.6 A2 to A3 and 120.12 A2 of the extant Code (the lead-in paragraphs) to recognize the potential for additional threat categories
Option 2	Build the missing concepts of complexity into the existing threat categories
Option 3	Add one or more new threat categories
Option 4	Highlight complexity as a pervasive factor in decision-making while applying the conceptual framework

13. These four non-mutually exclusive options were presented to survey respondents, with the highest support for options 1, 2 and 4:

Non-mutually exclusive	% "Yes" respondents	# "No" respondents
Option 1	66%	34%
Option 2	62%	38%
Option 3	53%	47%
Option 4	82%	18%

14. The Task Force noted that this mixed response is aligned with the preliminary views of IESBA members.

[3] A "strawman draft" of the potential revisions to the Code was included in the December 2020 agenda papers.

15. Respondents provided a variety of reasons as summarized in **Appendix 1** to explain their position:

- In general, those against incorporating complexity as a threat (whether it be Options 1, 2 or 3) believed that complexity is not a threat but arises from a lack of awareness or competence. Others were concerned about the potential unintended consequences of complexity as a threat, such as becoming a "catch-all" threat, and further questioned what the related safeguards would be. One respondent noted that "unknown unknowns" by nature require responses that cannot be prescribed.
- Those supportive of Option 1 (modifying the lead-in to 120.6 A2 to A3 and 120.12 A2 of the extant Code) thought that it was unrealistic to shoehorn all potential threats into five categories and that doing so would stunt the development of a PA's growth mindset.
- Those supportive of Option 3 (adding a new threat) or Option 2 (incorporating complexity in an existing threat) believed that today's complex and rapidly changing environment warrants complexity to be specifically recognized as a threat with appropriate safeguards.
- Those in support of Option 4 consider that complexity is not a threat per se, but rather a pervasive factor that should be considered when identifying and evaluating threats as it can cut across all threats and heighten threats in particular to professional competence and due care.

16. The Task Force further analyzed the unique combinations arising from the responses:

Unique combinations	# respondents	% of responses
Option 1 only	6	6%
Option 2 only	2	2%
Option 3 only	2	2%
Option 4 only	11	**12%**
Options 1 and 4	6	6%
Options 1 and 3	0	0%
Options 1 and 2	2	2%
Options 2 and 4	6	6%
Options 2 and 3	1	1%
Options 3 and 4	2	2%
Options 1, 2 and 3	5	5%
Options 1, 2 and 4	9	**10%**
Options 2, 3 and 4	1	1%
Options 3, 4 and 1	5	5%
All four options "Yes"	30	**32%**
All four options "No"	5	5%

Unique combinations	# respondents	% of responses
Total Responses	**93**[4]	**100%**

Key Themes Arising from the Above

17. PAs are generally experiencing the elements of complexity previously identified by the Task Force.

18. The top three examples of complexity most commonly provided by respondents are: technological transformation; understandability of laws and regulation; and cyber-security and privacy issues.

19. 26% of responses believe that there is a threat not captured in the Code; while at least 88 responses (95% of respondents) supported implementing at least one of the four options.

Case Studies

20. The survey had also included two case studies:

Professional Accountant in Public Practice (PAPP) scenario:	Professional Accountant in Business (PAIB) scenario:
The auditor's client uses an artificial intelligence system to estimate the valuation of a complex financial instrument. The algorithm uses deep learning. Initially, the calculations are similar to more traditional calculations but over time the artificial intelligence valuation of the financial instrument appears to be growing at a higher rate than expected by the auditor.	A professional accountant in business relies on a "black box" intelligent agent to determine an estimate in a high-stakes decision. The intelligent agent uses deep learning. Initially, the calculations are similar to more traditional calculations but over time the estimates from the intelligent agent appears to be growing at a rate that is not expected. The estimate becomes flawed, and the professional accountant's resulting decision leads to significant harm to the organization and the public.
Question: If the algorithm lacks explainability, the auditor might not be able to properly assess the extent to which evidence is sufficient and appropriate. In this situation, which threat(s) to which fundamental principle(s) would you identify? Please check any that apply.	Question: In this situation, which threat(s) to which fundamental principle(s) would you identify? Please check any that apply.

21. Observations:

- The number of responses to the two case studies were significantly lower than the responses to the other questions (PAPP: 32; PAIB: 15).

[4] Not all respondents provided a response to these questions.

- Given a range of 30 fundamental principle and threat combinations, including the category of "other" threat available, each combination was selected at least once.
- For both scenarios, the highest number of responses were selected for self-interest threatening compliance to the fundamental principle of Professional Competence and Due Care (PC&DC).
- For the PAPP scenario, high responses were also seen for familiarity threatening the fundamental principle (FP) of objectivity; and intimidation and "other" threatening PC&DC. The spread of threats elected under the PAIB scenario was more even.

III. THE IMPACT OF TECHNOLOGY ON AUDITOR INDEPENDENCE

Overview of Respondents

22. There were 50 responses to the Independence survey, including from 20 practitioners, 12 PAOs, 4 NSS, 4 academia, 2 investors, 2 regulators,[5] 2 Those Charged with Governance, 2 Other, 1 Preparer and 1 Unidentified.

23. Geographically, responses were spread across Asia-Pacific (12); North America (8); the United Kingdom (8); Africa (8); Europe (7); and South America (5) and global/unidentified (2).

24. In the summary of key themes presented below, the stakeholder group will only be specifically identified if the view was noticeably held by one group in particular. In most instances, views were supported by a mixture of stakeholder groups from a range of jurisdictions.

Context

25. The initial survey questions sought contextual information about the types of services or products made possible by advances in technology, and how these services or products have been developed and distributed.

26. The survey responses identified wide ranging services and products, with both high level functions and specific tools identified. New services or products identified included, but were not limited to:

    - Automation of key processes (transaction processing, control testing including cybersecurity, whistle blowing, analysis, reporting and checking).
    - Data analytics, AI document screening and predictive tools.
    - Data mining.
    - Blockchain-based functionality.
    - Hosting client data and ongoing monitoring.

27. Respondents identified a range of ways in which these services and products are developed, summarized in the following snapshot of responses:

    - 21% indicated jointly developed with a third party.
    - 12% indicated not jointly developed with a third party.
    - 67% indicated that service and products are jointly developed in some cases.

[5] One respondent provided feedback via a teleconference rather than via the survey template

28. Two respondents[6] commented that small or mid-tier firms tend to rely on third parties while the larger firms use bespoke inhouse developed tools. It was also noted that firms are at different stages.

29. A respondent[7] highlighted a need to explore independence considerations arising when technology is used that comes from someone who is closely linked to the client.

30. Respondents identified that these services are distributed to clients as follows:

    - 67% indicated by way of licensing agreement.
    - 57% indicated by way of service agreement.
    - 31% indicated "other".
    - 29% indicated through an outright sale.

31. The Task Force found that these responses confirmed prior discussions of the types of services and functions that are being made possible through advances in technology. This context was helpful in light of the diagram previously developed by the Task Force (included as **Appendix 2**) to categorize the evolving technology tools and non-assurance service (NAS) engagements. This categorization would then help assess how Section 600 and its sub-sections might address such new tools and services.

32. The more detailed results did provide some use case examples. The Task Force has shared the detailed survey results with the Technology Working Group as they consider the development of non-authoritative guidance material (NAM).

Key Themes Identified

Application of NAS Provisions Where a Firm Sells or Licenses Technology that Performs a NAS

33. 76% of respondents agreed with the question, "Do you consider that the independence requirements that apply to the provision of NAS to an audit client (e.g., Section 600 and its subsections) to identify, evaluate and address the threats to independence are relevant where the firm sells or licenses technology that performs a NAS?".

34. This view from a substantial number of the respondents was supported by the following key messages:

    - Activities performed by technology are considered to be a NAS delivered by the firm in an automated fashion.
    - The same principles should apply regardless of whether the service is performed by a person, by technology or both. In assessing the permissibility of the service, the nature of the underlying service is evaluated to identify whether a management responsibility is assumed or a self-review threat arises.
    - Support for a principles-based approach. Specific technology-related provisions will risk becoming obsolete.

[6] A professional accountancy organization and a regulator

[7] A regulator

35. One respondent[8] did identify a potential additional factor to evaluate, namely whether a management responsibility is assumed, i.e., whether management has sufficient understanding of and interaction with technology (e.g., algorithms) to take responsibility.

36. A respondent[9] noted that an independence threat might not arise immediately where an audit firm uses technology for audit purposes. However, there is a risk that over time, the insight from these tools increases the threats to independence, and that firms need to be aware of this increasing threat.

37. Some respondents did highlight:

    - A need to consider the different ways in which firms use technology and to demonstrate how the NAS provisions apply given that the sale or licensing of technology is not covered explicitly, but rather covered in principle, by paragraph R600.4.[10]
    - That while they consider that the NAS provisions appropriately apply to technology, they are seeking NAM, for example frequently asked questions, to illustrate how.
    - Merit in adding application material in the NAS section to address technology more explicitly.

38. One respondent[11] raised the need to consider whether the sale or licensing of technology is similar to the case of loaned staff.

39. The Task Force was particularly interested that 24% of respondents, including a range of stakeholders (practitioners, NSS, PAOs and a preparer) from a range of jurisdictions, did not agree that the NAS provisions apply where a firm sells or licenses technology that performs a NAS. No reason was provided for this view. The Task Force observed that some of these respondents recommended the addition of new paragraphs to deal with simple business relationships, and both the buying and selling of goods.

40. A number of respondents recognized that a business relationship is created by the sale or licensing of technology, especially where technology is developed by another party, or where there is ongoing support.

41. 31% of respondents responded yes to the question, “Have you developed any policies, procedures or guidance for these services or technology regarding identification, evaluation and addressing threats to independence created through the provision of these services?”.

42. A few respondents stressed their view that to maintain independence, it is important that firms do not sell or license technology to audit clients.

Product versus Service Continuum

43. In response to the question “Considering the product-to-service continuum, are you aware of any pure products (i.e., products without a related NAS element?),” a substantial number of respondents

---

8 A practitioner, auditor or audit firm

9 A regulator

10 Paragraph R600.4 of the extant Code explains that before a firm or a network firm accepts an engagement to provide a non-assurance service to an audit client, the firm shall determine whether providing such a service might create a threat to independence.

11 A practitioner, auditor or audit firm

considered that there is no need to categorize a technology tool as a "product" or a "service." This is in line with the Task Force's view. In addition:

- 83% were not aware of any pure products.
- 17% indicated there are pure products without any NAS.

44. The Task Force was specifically interested in the examples identified by respondents of "pure" products which included:

- Technology that provides generic information, but that cannot be relied upon as advice.
- Technology that has no impact on financial systems and controls. Some examples described include an app to reduce the spread of COVID-19 or a customer relationship management tool.
- Reselling products developed by a third party where the audit firm acts as distributor or agent.

Should Section 600[12] and Its Subsections be Amended?

45. Themes emerging from those respondents who were looking for the NAS section to cover technology more specifically included:

- Software as a service.
- Address upfront in Section 600 in the general definition of a service so as to minimize change.
- Technology used for audit purposes that creeps into providing consulting services.
- Multiple contracting parties.
- When a non-audit client becomes an audit client.
- Collecting, storing and hosting client data for economic benefit.
- The frequency of the service performed and ongoing support maintenance and updates.
- Non-financial reporting.

46. Mixed views were expressed in response to the question, "Are there services enabled by technology advances that you believe should be more specifically covered in the independence requirements (e.g., by more specifically including them in subsections 601-610 or in their own sub-sections)?":

- 57% responded no.
- 43% responded yes.

47. Some suggestions identified by respondents who responded "yes" include, but are not limited to:

- Consider each subsection in light of advances in technology, e.g., Internal control services.
- Digital ledger/blockchain.
- Any additional NAS emerging.

48. A number of the ideas expressed by respondents had been discussed by the Task Force. At the December 2020 IESBA meeting, the Task Force:[13]

[12] Section 600, *Provision of Non-Assurance Services to an Audit Client*

[13] IESBA December 2020 Agenda Item 5-A

- Recommended adding wording within the introduction of Section 600 to make it explicit that a NAS might be performed by individuals within the firm, by technology owned by the firm, by technology sold or licensed by the firm to the client, or a combination thereof.
- Recommended not to include a separate section to cover technology-enabled NAS as a broad category. In many instances, technology-enabled services relate to existing service categories.
- Recommended adding more parts to Subsection 606[14] to cover Operations, Maintenance, Monitoring or Support and Hosting.
- Recommended that the examples in the NAS sections are already sufficiently broad to cover and include services that are increasingly augmented or performed by technology. The Task Force noted that NAM might be a more appropriate way to address any calls for more guidance.
- Explored whether there is a need for a new subsection, for example whether blockchain enables new services (such as eCommerce support) or whether it is enabling existing services (such as bookkeeping) through the use of a digital ledger. The Task Force was hoping that the survey results would assist in determining the need for a new subsection and has noted mixed views in response to this issue.

Clarification of Subsection 606

49. In response to the question, "Do you believe that the independence requirements relating to information Technology System Services (e.g., in Section 606) would benefit from additional clarity on the following matters", there was strong support for clarification of Subsection 606:
    - 75% supported clarification of what "implement and design" mean.
    - 75% supported clarification of what "customization" and "configuration" mean and how they differ.
    - 63% supported clarification of what "off the shelf" constitutes.
    - 63% supported clarification of what would be considered as "not significant" levels of customization.
    - 23% supported other clarifications of Subsection 606. Suggestions included addressing: blockchain, hosting, clarification of the evaluation of financial and non-financial systems.
50. Those respondents who did not believe that it is necessary to amend the Code tended to suggest that these matters might best be dealt with in NAM.
51. The Task Force found these responses helpful to reflect on prior deliberations outlined by the Task Force at the December 2020 IESBA meeting,[15] where the Task Force recommended the following:
    - There was no need to define "information technology systems."
    - Limiting the amount of change to Subsection 606 (i.e., the Task Force did not recommend covering each stage of installation, configuration, customization and integration in detail in the Code).

[14] Subsection 606, *Information Technology Systems Services*

[15] IESBA December 2020 Agenda Item 5-A

- That more guidance is needed on customization as it relates to "off-the-shelf" software.
- That the term "configuration" better describes "insignificant" customization that involves no modification of the software coding. As such, a different term was suggested for clarification in paragraph 606.3 A1.

52. In terms of the detailed narrative provided by respondents,[16] some additional points identified for consideration include, but were not limited to:

- The need for clarity regarding management's role and extent of capability to oversee any design.
- Autonomy of the technology where the need for human judgment is less relevant.
- A need to clarify what is a financial versus non-financial system, noting advances in integrated systems.

Business Relationships

53. There were mixed views in response to the question, "In what circumstances do you consider that selling or licensing technology to a client creates a close business relationship (such as those in 520.3 A2, and would warrant prohibition (such as in R520.4)?".

54. Some respondents acknowledged the business relationship, albeit not necessarily a close business relationship, or conflict of interest arising from the sale or licensing of technology. They expressed a desire for the Code to address the sale of products more explicitly, e.g., for Section 520[17] to address both the buying and selling of goods to an audit client.

55. A few respondents identified factors to consider in determining whether a licensing arrangement is considered a close business relationship, including:

- Is the licensing arrangement a significant part of the services provided.
- The extent to which the firm has been involved in the development.
- Whether the arrangement is bespoke to the client.
- How revenue is generated, and whether the amount is material.
- Whether the client is the end user or not.

56. Others considered that:

- The existing requirements in 520.3 A2 and 520.4 cover this well.
- Evaluating a digital offering as a business relationship is not the appropriate starting point.
- Licensing technology does not generally create a close business relationship that warrants a prohibition, but that the substance of each relationship needs to be considered.

57. One respondent[18] noted that the sale and licensing of technology would create a close business relationship in all instances and should always be prohibited.

---

[16] Practitioners, auditors or audit firms

[17] Section 520, *Business Relationships*

[18] A practitioner, auditor or audit firm

58. The Task Force has previously explored with the IESBA various approaches to address any business relationship arising from the sale or licensing of technology.

59. In September 2020,[19] the Task Force invited comment from the Board on the need to evaluate threats to independence arising based on the business relationship that is formed through the arrangement. Extracts from the September meeting minutes note that some Board members expressed concern that the Task Force viewed the simple existence of a software license as constituting a business relationship. It was noted that a business relationship only exists where there is a mutuality of interests between two parties, for example when both parties work together to drive business through an alliance. The Task Force believes that the terms business relationship and close business relationship should be more clearly differentiated as it appears to create confusion.

60. In December 2020,[20] the Task Force sought feedback on an amended approach to clarifying Section 520, with a focus on adding examples of a close business relationship that might result from the sale and licensing of technology with a focus on mutuality of interest examples. The Board expressed general support for a focus on the examples of what is considered mutuality of interest. However, some Board members expressed concern that the draft examples were too complicated and specific.

"Routine or Mechanical"

61. 78% of respondents agreed with the question, "Do you agree that the key determining factor as to whether a task is "routine or mechanical" is whether the task requires little or no technical expertise or professional judgment, rather than whether the task can be automated so as to be executed in a "routine or mechanical" manner?" This aligns with the Task Force's previously stated view that the key determining factor as to whether a task is routine or mechanical is whether it requires little or no technical expertise or professional judgment.

62. 22%[21] did not agree with this view. One respondent[22] commented that anything that is done by software is repetitive, so this would be considered to be "routine and mechanical."

63. Some of the factors identified when considering whether automated services, including those enabled by machine learning, are routine or mechanical included, amongst others:

- Whether it is performed by "off the shelf" software, with little or no customization.
- Client documentation.
- How repetitive the action is, i.e., is it the same every time.
- The need for a decision, expertise or learning.
- Management responsibility.
- Complexity.

---

19 IESBA September meeting Agenda 7-A

20 IESBA December 2020 Agenda Item 5-A

21 Expressed by some practitioners, one academic and by the only investor or user of financial statements respondent

22 A practitioner, auditor or audit firm

64. At the September 2020 meeting,[23] the Task Force recommended retaining the term "routine or mechanical." The Task Force has developed additional application material, in conjunction with the NAS Task Force, highlighting that it is the level of professional judgment that is a key determining factor in assessing whether a service is routine or mechanical.

NEXT STEPS

65. The Task Force intends to continue to deliberate on the feedback received from these surveys, from CAG Representatives and the Board as it works to develop a technology-related ED.

66. The Task Force anticipates presenting an update on some of the recommendations at the June 2021 IESBA meeting.

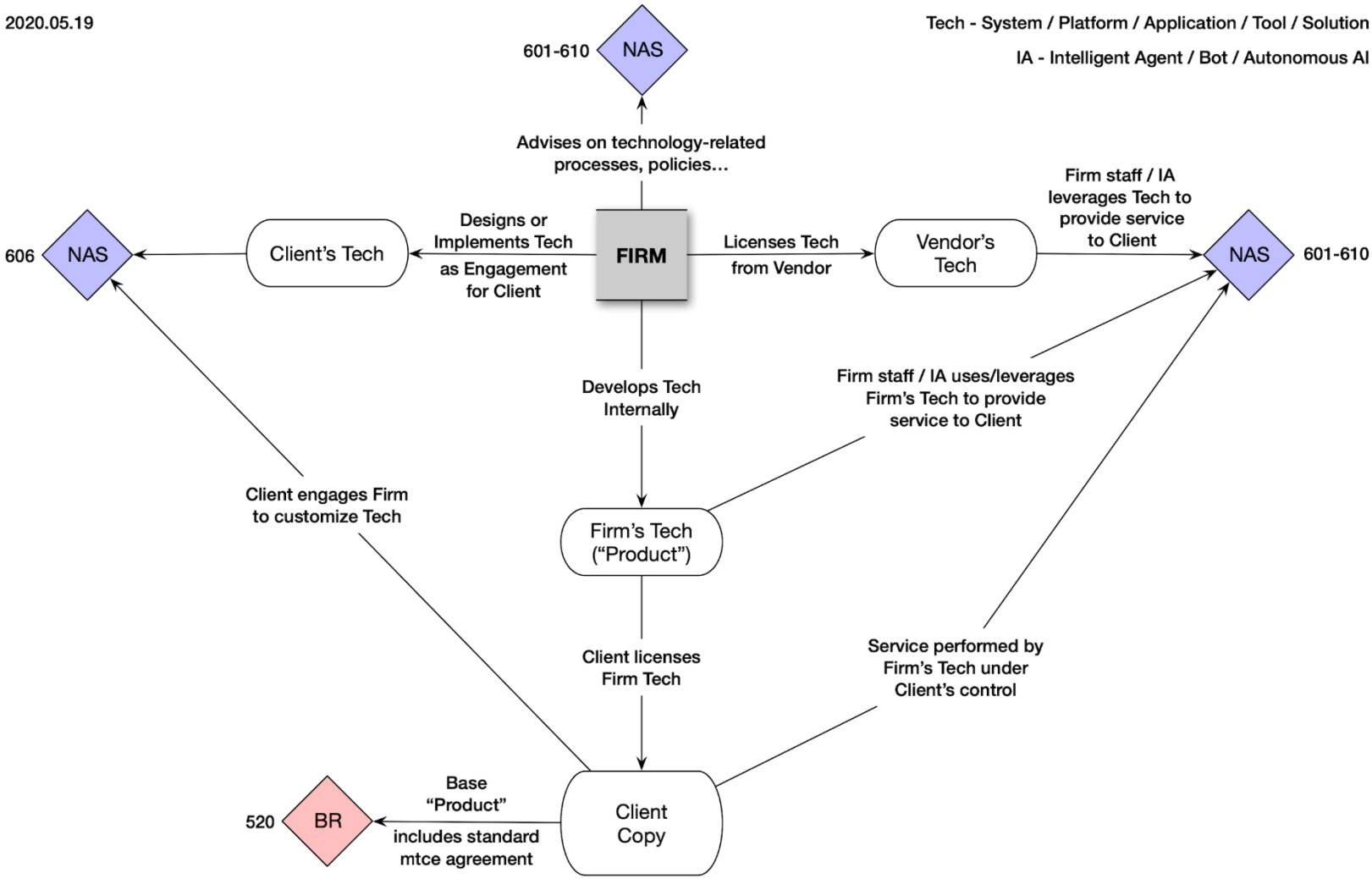
[23] IESBA September meeting Agenda 7-A

Appendix 1

	Key themes for "Yes"	**Key themes for "No"**
Option 1: Modify lead-in	• Not possible to centrally define all threats, necessitating the need to be open minded as to the general possibility of unknown unknowns. • Unrealistic and underestimates the business environment. • PAs need to develop a questioning mindset and to be actively thinking of all types of threats – not just accepting there are "five". • The understanding of threats and the categories might differ in jurisdictions and cultures.	• Unclear why cognitive or other new technologies introduce threats that are not compatible with existing ones. • Would lead to: (i) significant effort; (ii) duplicative considerations; (iii) inconsistent application; and (iv) uncertainty in determining an appropriate safeguard. • PAs would need examples and factors to evaluate potential other threats. • With more nuances added, there could be risk of national bodies diverging when adopting in their own ethics codes.
Option 2: Amend existing threat	• May steer the practitioner to prepare documentation and/or consult to a greater degree. • Allows for a consistent interpretation of what is complexity.	• Threats are different from complexity. Complexity may arise from a lack of awareness of the technology. • Potential unintended consequences of changing existing threats which are well known in the profession. • Non authoritative guidance can allow for education.
Option 3: Add a new threat	• Impact of the COVID-19 global pandemic, new technologies, sustainability and climate change create new areas of risk deserving their own separate category to be adequately identified, measured and mitigated. • Prompts PAs to continuously consider the impact of evolving complexity, aligned with the Role and Mindset revisions as well as ISA 540 (Revised).[24]	• Unknown unknowns by their nature require responses that cannot be automated in line with a template. • Complexity is not an actual threat, but a factor to consider. • Potential unintended consequences such as from the perspective of practical implementation of a safeguard. • Adding a particular threat for complexity might make PAs overlook other threats and/or risk becoming a "catch-all".
Option 4: As a factor to consider	• Complexity should be a factor when identifying and evaluating threats as it can heighten threats in particular to professional competence and due care.	• Complexity has always been a factor in making professional judgments. It should not now become an additional pervasive factor.

[24] ISA 540 (Revised), *Auditing Accounting Estimates and Related Disclosures*

Appendix 2


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