Agenda Item 19 (a) – Summary of Submissions on the IESBA Technology ED and Task Force Responses

The following provides a high-level summary of comments on the IESBA Technology ED on six significant issues identified and the Task Force's preliminary responses (Agenda Item 8). The IESBA Task Force's preliminary proposed changes (marked-up) are in Agenda Item 8B.

o *Professional Skills (Section 113)*

The respondents had mixed views on the proposed addition of *'interpersonal, communication and organisational skills'* to emphasise the professional skills that professional accountants (PAs) need (proposed paragraph 113.1 A1 of the IESBA Technology ED) with 'fairly reserved support' for this change.

Some respondents believe such skills are generic and not specific or relevant to technology and the soft skills required for the PAs vary depending on their roles. Respondents also believe that the soft skills added are an incomplete list and should consider other technology-relevant skills, such as technical competence, professional skills and professional values, ethics and attitudes.

The Task Force propose to revise paragraph 113.1 A1 by removing the list of soft skills and adding them to a new paragraph 113.1 A2 which also:

▪ Reflects the scalability of the level and types of skills required and that this depends on the PA's role;

▪ Emphasises that the soft skills listed are examples only and not a complete list; and

▪ Highlights that technology-based knowledge is also relevant to competence.

o *Confidentiality (Section 114)*

The IESBA Technology ED included a prompt in proposed paragraph 114.1 A1 for PAs to secure confidential information throughout the data governance lifecycle and a proposed new definition of 'confidential information'. Respondents supported the proposal on securing information, however, with some suggestions for further guidance or clarification, including the expectation of a PA in scenarios where information is unlawfully disclosed.

Respondents sought further clarity regarding the proposed definition of confidential information, such as on the term 'public domain' and the scope of confidential information. Respondents also noted complying with confidentiality in an employing organisation includes sharing responsibility with other employees.

The IESBA Task Force propose new provisions, including:

▪ a requirement for PAs to maintain confidentiality even if aware that confidential information has been improperly disclosed (R114.1(h)).

▪ guidance for PAs to consider laws/regulations in jurisdictions where disclosure might take place (114.1 A3).

▪ guidance on factors to consider when providing confidential information with the consent of the provider (114.1 A4).

The IESBA Task Force also proposes replacing "secure" with "protect the confidentiality of" in paragraph 114.1 A1 and "public domain" with "is not publicly available" in the definition of confidential information and incorporating changes to recognise employing organisation's internal controls and approach to technology issues.

○ *Complex Circumstances (Section 120)*

The IESBA Technology ED included guidance on relevant facts and circumstances that might give rise to complex circumstances and how this might be managed by PAs. The respondents expressed mixed views on these proposals.

Some respondents raised concerns about the vagueness of the guidance and that it is unnecessary to include it in the Code as complying with the fundamental principles does not require a distinction between complicated and complex circumstances. It was also noted that the concept of 'complexity' should be aligned with how it is addressed in ISA 315 (Revised) *Identifying and Assessing the Risk of Material Misstatement,* which includes complexity as one of the inherent risk factors. Another suggestion was complexity should be incorporated as a factor to consider when evaluating threats to the fundamental principles.

Other respondents supporting the proposals suggested:
- incorporating examples of complex matters in the Code (including APESB's comment);
- material explaining the distinction between complicated and complex; or
- other factors to manage complexity include documenting uncertain elements, multiple variables and assumptions and how they are interconnected or interdependent (APESB suggestion).

The IESBA Task Force noted the respondents varied understanding of the term 'complex' and propose to relocate this material to follow material on exercising professional judgement (a move to paragraphs 120.5 A6 and 120.5 A7). The Task Force also propose to enhance the material for understandability and add a new factor about analysing and investigating uncertain elements, multiple variables and how connected or interdependent.

○ *Use of Technology (Sections 200, 220, 300 and 320)*

Respondents generally supported the additional factors proposed in the IESBA Technology ED to assist in identifying threats to the fundamental principles when PAs rely upon the output from technology (220.6 A2 and 300.6 A2). However, respondents raised various concerns, including:
- considerations should be linked to specific threats.
- whether it is reasonable to expect PAs to have sufficient expertise or understanding to use the technology – access to an expert that does should be regarded as equivalent.
- the consideration "*whether technology incorporates expertise or judgements of the accountant or the employing organization/ firm*" requires clarification (including APESB's comment on this).

2

- several other considerations relevant to identifying threats should be included.

- Safeguards, such as third-party certifications, compliance with recognised technology standards and periodic reviews, should be added.

Respondents also generally supported the factors for PAs to consider as to whether reliance on the output of technology is reasonable or appropriate for the intended purpose (220.7 A2 and 320.10 A2). However, regulators had some reservations, including that technology should be in a separate section from "Using the Work of an Expert" and the emphasis should be on the whole process, not just the output. Other respondents sought clarification on factors, or the addition of other factors.

The IESBA Task Force proposes revisions to relevant paragraphs, including:

- Adding subheadings "Identifying Threats Associated with the Use of Technology" and listing specific threats in paragraphs 200.6 A2 and 300.6 A2.

- Adding a circumstance that the "data available is not sufficient for the effective deployment of the technology" relating to self-interest threat (200.6 A2 and 300.6 A2).

- Amending the circumstance around professional competence to "the accountant does not have sufficient expertise, or access to an expert with sufficient understanding" (200.6 A2 and 300.6 A2).

- Amending the consideration "*whether technology incorporates expertise or judgements of the accountant or the employing organization/ firm*" to "*use of the technology requires the knowledge, expertise or judgements of the accountant or the employing organisation/firm*" (paragraphs 200.6 A2 and 300.6 A2).

- Creating a separate subsection in 220 and 320 on "Using the Output of Technology" and relocating and making requirements specific to when the PA intends to use the output of technology, they must exercise professional judgement to ensure it is reasonable or appropriate (R220.8 and R320.11).

- Amending paragraphs 220.8 A1 and 320.11 A1 on the factors to consider when intending to use the output of technology to address respondents' concerns.

o *Close Business Relationships (Section 520)*

The IESBA Technology ED included a prompt in Section 520 of the IESBA Code to consider the relevance of the non-assurance services (NAS) in Section 600 when technology is provided, sold, resold or licensed by a firm to its audit clients. Most respondents supported this signpost. However, some respondents expressed the view that NAS and business relations are very different and will create confusion. The IESBA Task Force disagree with this concern and believe the signpost to Section 600 is necessary.

The IESBA Technology ED also included an example of a close business relationship arising from the provision of technology. There was general support from respondents on this, and some suggested other examples and a general principle for identifying or assessing a close business relationship. The IESBA Task Force propose:

- expanding the signpost in Section 520 to Section 600 so that it includes indirect services such as the development of software by firms for non-audit clients that then use this software in services provided to the firm's audit clients; and

- highlighting arrangements where firms license products to or from clients as potentially creating close business relationships.

o *Hosting (Subsection 606)*

The IESBA Technology ED included a prohibition on services relating to the hosting (directly or indirectly) of an audit client's data. Most respondents were supportive. However, some were of the view that the proposal is too broad and does not consider the nature of the data and the hosting service provided.

The IESBA Task Force considered the comments and revised the material concerning hosting in paragraph 606.3 A1 to be more specific on the types of prohibited hosting services. The phrase 'services in relation to hosting' is proposed to be replaced with 'stores data or manages' to be more specific to the hosting services prohibited and to introduce (a) to (c) with examples of when a specific method or purpose of hosting would result in management responsibility and clarify that it does not cover the hosting of all data.