Ernst & Young Australia Operations Pty Limited
200 George Street
Sydney NSW 2000 Australia
GPO Box 2646 Sydney NSW 2001

Tel: +61 2 9248 5555
Fax: +61 2 9248 5959
ey.com/au

19 October 2020

The Chair
Accounting Professional Standards & Ethical Standards Board
Level 11
99 William Street
Melbourne VIC 3000

Dear Ms Milne,

Exposure Draft 02/2020 – Proposed revisions to APES 305 Terms of Engagement

Ernst & Young ("EY") welcomes the opportunity to comment on the Exposure Draft 02/2020 ("ED").

EY considers that there are a number of fundamental conceptual matters which need to be clarified with respect to the scope and practical application of the proposed revisions. We strongly urge the APESB to address these issues prior to releasing the updated APES 305 *Terms of Engagement* ("APES 305") in its final form.

Outlined below are our specific observations and recommendations on the proposed revisions to APES 305 as outlined in the ED.

1. **Further clarification is required on the depth and breadth of application of the proposed revisions to Cloud Computing**

It is not clear which Cloud Computing services require mandatory disclosure pursuant to paragraph 3.6, optional disclosure pursuant to paragraph 3.7 or no disclosure at all. Furthermore, the ED provides no details on the "nature" and "extent" of such disclosures. In its current form, the ED contemplated that almost every Cloud Computing application used in service delivery is required to be or should be disclosed to the client.

> *3.6 Where a Member in Public Practice utilises Outsourced Services in the provision of Professional Services to a Client the Member shall document and communicate the details of the Outsourced Service Provider, the geographical location of where the Outsourced Services will be performed and the nature and extent of the Outsourced Services to be utilised.*
>
> *3.7 Where a Member in Public Practice utilises Cloud Computing in the provision of Professional Services to a Client which is not an Outsourced Service, the Member in Public Practice should document and communicate to the Client the details of the Cloud Computing provider, the geographical location of where the Cloud Computing will be performed, where Client data will be stored and the nature and extent of the Cloud Computing to be utilised.*

We provide below further analysis of the issues that we have identified.

Building a better working world

1a. Issue - Cloud Computing examples in APES GN 30 Outsourced Services have not been updated

In order to implement paragraphs 3.6 and 3.7 the Member should refer to the definitions and the examples in APES GN 30 *Outsourced Services.* The examples regarding Cloud Computing date back to the original APES GN 30 in 2013. The use of Cloud Computing has become increasingly ubiquitous and the examples do not address the various scenarios in which Cloud Computing is used. For example large firms may use internally developed global applications, Members may use off-the-shelf professional services packages and other ubiquitous software applications that are not industry-specific applications but are none-the-less cloud-based and used in the delivery of professional services. Some of these applications are integral to service delivery whilst others are peripheral applications that are not integral but nonetheless may process and/or retain client information in some form.

1a Recommendation

We recommend that:

- The APESB canvas Members across different sized practices to understand the nature in which Outsourced Services and Cloud Computing are being used.
- The examples in APES GN 30 *Outsourced Services* should be updated to reflect the information provided by the Members canvassed.

We believe that the updated examples will serve as a more robust framework for Members to apply APES 305 together with their own judgement to determine disclosure and the "nature" and "extent" of such disclosure to the client. Sections 1b to 1d below provide examples of applications which we recommend the examples in APES GN 30 *Outsourced Services* should address.

1b. Issue - Internally developed software integral to service delivery – in scope for paragraph 3.6?

EY as a member of the global network of Ernst & Young firms (each of which is a separate legal entity) has invested heavily in technology platforms and tools in recent years and uses internally-developed software applications that are in some cases hosted by a third party Cloud Computing service provider. Some of these applications are integral to delivery of a service to a client and arguably satisfy the definition of a Material Business Activity. Having regard to the last sentence in the definition of Material Business Activity, clarification is required on whether such applications would indeed satisfy the definition of a Material Business Activity that is an Outsourced Service and therefore require disclosure pursuant to paragraph 3.6.

> ***Material Business Activity*** *means an activity of an entity or a Firm that has the potential, if disrupted, to significantly impact upon the quality, timeliness or scale of Professional Services offered by a Member in Public Practice or received by a Client. Whether a business activity is a Material Business Activity should be based on an assessment of the risks associated with the nature and size of the activity and the business activity's relevance to the Professional Service delivered to the Client. Material Business Activities exclude the internal activities of a Firm such as record storage or software application hosting where these internal activities merely support the Professional Services delivered to the Client.*

EY also utilises third-party cloud-based global technology platforms that enable our client serving professionals to access the latest tools, templates and a library of internal and external reference materials. Whilst its content is integral to service delivery, it contains no client data, it is arguably a Material Business Activity that would require disclosure pursuant to paragraph 3.6.

Many of EY's non-audit services have broad suites of primarily internally-developed software tools that are cloud-based and sometimes hosted by third parties. As a global network of firms, new global tools are continually being developed. At the point of execution of the engagement agreement it is sometimes difficult to ascertain which tools will be used, as part of the service delivery, given that this can be determined based on factors which may occur or change as the engagement progresses, for example scope changes. If such tools are integral to service delivery then the application of paragraph 3.6 would require the EY team to include in the engagement agreement a comprehensive list of every tool that could potentially be used, the name of the Cloud Computing service provider and server location. Including such a standardised list as part of the engagement agreement would not however address the mandatory "nature" and "extent" disclosure requirements of paragraph 3.6. Please see section 2 in this letter for further discussion on practical issues around disclosure of "nature" and "extent".

1c. Issue - Off-the-shelf cloud-based software integral to service delivery – in scope for paragraph 3.6?

Members may use cloud-based software such as MYOB and Xero as Material Business Activities in their service delivery. Both of these applications are hosted on Microsoft Azure cloud solution. Pursuant to paragraph 3.6, it appears the Member is required to identify in the engagement agreement the software package, the software package's cloud service provider and server locations. If so, then when the Member changes software package during the course of the engagement, this would suggest that the Member would be required to reissue the engagement agreement. Similarly, when the software package provider itself changes cloud host, this interpretation would suggest that the Member would be required to reissue the agreement.

1b and 1c Recommendations

We recommend:

- The last sentence in the definition of Material Business Activity should be refined to clarify which platforms are Material Business Activities.
- APES 305 should clarify that paragraph 3.6 does not require the disclosure of every conceivable outsourced Material Business Activity in the engagement agreement.
- That the engagement agreement state that client information may be provided to external service providers however the Member shall be responsible for maintaining the confidentiality of client information regardless of by whom such information is stored on the Member's behalf.

Building a better working world

Based on recent engagement agreement discussions with clients, in our experience most clients seek overarching assurance and acknowledgement from the Member of their responsibilities in this regard instead of a granular analysis of the nature and extent to which Outsourced Services and Cloud Computing are used. For those clients that require further clarification on data security, the Member's IT security team would typically address the client's data security concerns with the client's own IT security team. Articulating such IT related matters is beyond the scope of most Members and will potentially make the preparation and execution of the engagement agreement burdensome, to both the Member and the client.

1d. Issue - Peripheral Cloud Computing packages – prima facie wide array of packages in scope for disclosure pursuant to paragraph 3.7

Below are just a few examples of cloud-based applications that are not Material Business Activities but are used in relation to client service delivery and could potentially contain "client data" which is not defined in the ED:

- EY specific example: Global Engagement Agreement Repository to store executed engagement agreements

- EY specific example: Process for Acceptance of Clients and Engagements for efficiently coordinating client and engagement acceptance, as well as continuance activities in line with firm policies and professional standards.

- Microsoft Office 365 suite which has various subscription levels offering different cloud hosting options.

- Outlook email application that is included in the Microsoft Office 365 suite and can be accessed via mobile phone.

In our view it is not beneficial or meaningful to a client, pursuant to paragraph 3.7, that Members individually identify and communicate to the client every Cloud Computing application that could potentially contain information related to the client.

1d. Recommendations

In light of the complexity and potentially broad remit of Cloud Computing, we recommend that:

- APES 305 clearly identify which Cloud Computing applications fall withing the scope of APES 305.
- APES 305 should include a definition of "client data" in the context of Cloud Computing.

As previously stated, updated examples in GN *Outsourced Services* can serve as a framework for Members to refer to in determining the scope. If a scope periphery cannot be established then paragraph 3.7 should not be included in APES 305. The unintended consequence of this requirement will be a disclosure standard that many Members will find unachievable in practice.

Building a better working world

Consistent with Recommendations for 1b and 1c, we recommend:

- APES 305 should make it clear that paragraph 3.7 does not suggest Members disclose every conceivable Cloud Computing provider in the engagement agreement.
- There is a requirement in the engagement agreement to include a general statement that client information may be provided to external service providers however the Member shall be responsible for maintaining the confidentiality of client information regardless of by whom such information is stored on the Member's behalf.

2. Issue - Mandatory disclosure of the nature and extent of Outsourced Services to Clients pursuant to paragraph 3.6

There are practical issues with the required disclosure for the "nature" and "extent" of Outsourced Services, including:

- The engagement agreement is ordinarily executed prior to the commencement of the actual engagement work and the planned "nature" and "extent" of the utilisation of the Outsourced Services may not be fully known in order to be formally communicated at this stage. Indeed, an engagement agreement could span multiple years and specific procedures may be refined for non-audit services as the engagement progresses.
- The extent of the services outsourced may evolve as more information is received throughout an engagement. It is impractical to obtain agreement from a client each time the scope of the Outsourced Services alters and when information is obtained. For example, in an audit engagement using cross-border teaming arrangements, the local audit engagement team would be making an assessment throughout the engagement on whether to use other Network Firms to assist in audit procedures based, amongst other things, on project management considerations like the nature and timing of the information provided by the client and local staff availability.
- The level of detail and complexity involved may differ between engagements which would hinder a standardised approach to documenting the "nature" and "extent" of Outsourced Services.
- Compliance costs to documentation of "nature" and "extent" of Outsourced Services to each client where such services occur on a frequent basis.
- Influencing the content of engagement agreements agreed in other jurisdictions would be particularly challenging given there is no international equivalent requirement.

2. Recommendations

Considering the practical issues around the disclosure of "nature" and "extent" by the Member at the date of the engagement agreement and throughout the engagement, we recommend:

- The mandatory requirement to disclose the "nature" and "extent" pursuant to paragraph 3.6 is removed.

As stated above, in our experience most clients seek overarching assurance and acknowledgement from the Member of their responsibilities regarding confidentiality and security of information instead of a granular analysis of the nature and extent to which Outsourced Services and Cloud

Computing are used. For those clients that do request further information on Outsourced Services or Cloud Computing, the Member should cooperate with the client in this regard, including deferring to the Member's IT security expert when appropriate.

3. Issue - Confidentiality in paragraph 3.4

The ED includes the following new paragraph on confidentiality, reasserting the existing requirement in APES 110 *Code of Ethics for Professional Accountants (including Independence Standards)*:

> *3.4 A Member in Public Practice who acquires confidential information in the provision of Professional Services to a Client shall comply with Subsection 114 Confidentiality of the Code including not disclosing confidential information to a third party without proper and specific authority from the Client unless there is a legal or professional duty or right to disclose.*

It is unclear whether paragraph 3.4 operates to limit the means for obtaining the client's authority to the engagement agreement and therefore the timing of such authority to the engagement agreement phase. There are scenarios outside the engagement agreement phase that would require the Member to seek such authority. For example, after the provision of the service, a third party may request a copy of the report deliverable prepared by the Member for the client. In such circumstances, the means for obtaining the client's authority will ordinarily be a letter signed by the client consenting to the release of the report.

3. Recommendation

To avoid the potential misinterpretation of APES 305 *Terms of Engagement* mandating the means for obtaining the authority specified in APES 110 *Code of Ethics for Professional Accountants (including Independence Standards)* we recommend:

- Paragraph 3.4 is removed from APES 305 *Terms of Engagement*.

4. Issue - Consistency with international standards and interaction with existing Australian professional standards and legislation

The International Ethics Standards Board of Accountants ('IESBA') has not issued an equivalent pronouncement to APES 305 or its sister guidance statement APES GN 30 *Outsourced Services*.

Members in Public Practice are required to maintain quality control and manage risk in the delivery of professional services in accordance with a variety of existing professional standards, including but not limited to standards and guidance statements issued by the Auditing and Assurance Standards Board (AUASB) which has issued ASQC 1 *Quality Control for Firms that Perform Audits and Reviews of Financial Reports and Other Financial Information, Other Assurance Engagements and Related Services Engagements* and ASA 210 *Agreeing the Terms of Engagements* and the Code of Professional Conduct contained in the Tax Agent Services Act 2009 (Cth). Also, in the context of audit quality, several audit firms are subject to audit inspection by ASIC on a periodic basis, and by CAANZ in relation to quality control practices.

Building a better working world

In addition to the lack of consistency with international standards, the proposed revisions to APES 305 impose additional requirements which extend responsibilities beyond those under existing Australian professional standards.

In drafting the proposed revisions to APES 305, the APESB has considered APRA Prudential Standard CPS 231 *Outsourcing*, guidance in TPB(PN) 1/2017 *Cloud computing and the Code of Professional Conduc*t and the Australian Privacy Principles in the *Privacy Act 1988*.

CPS 231 requires an APRA-regulated institution to consult with APRA prior to entering into agreements to outsource Material Business Activities to service providers that conduct their activities outside Australia; and notify APRA after entering into agreements to outsource Material Business Activities. Considering the existing framework of professional standards and legislation applicable to Members, and that CPS 231 specifically relates to the interaction of financial institutions with their regulator, in our view it is not appropriate to apply the APRA-derived concept of Outsourced Services to accounting firms providing professional services to require disclosure of these arrangements to their clients.

The Tax Practitioners Board (TPB) released TPB(PN) 1/2017 *Cloud computing and the Code of Professional Conduc*t, which provides useful guidance for registered tax practitioners in relation to Cloud Computing. The TPB guidance relevantly notes (at paragraph 10) that in determining whether Cloud Computing arrangements involve the disclosure of client information to third parties, it requires you to recognise that "*there is a distinction between data storage that a third party cannot effectively access (for instance, through the use of encryption) and disclosure to a third party*." Where client consent is required it is recommended (not mandatory) that the registered practitioner clearly inform the client about the proposed disclosure (including noting to whom and where the disclosure will be made, and where data will be stored) and a general authority consenting to disclosure to third parties may also be acceptable (paragraph 12).

To the extent Members are required to comply with the *Privacy Act 1988*, given this is existing legislation, our view is such Members will already have procedures in place.

4. Recommendations

We recommend:

- The development of a consistent international approach.
- APES 305 adopts a consistent approach with TPB(PN) 1/2017 in relation to disclosure requirements for Cloud Computing.

Outsourcing is neither new nor unique to firms in Australia and we see no current need for Australia to mandate requirements outside of the international framework or existing professional standards and legislation, resulting in additional jurisdiction specific conditions in Australian engagement agreements.

Building a better working world

5. Proposed operative date and transition recommendations

We recommend:

- In respect of the proposed operative date, APES 305 provide clarification in relation to "engagements commencing".
- Revised APES 305 only apply to engagement agreements that are entered into on or after the operative date, as there may be situations where services may commence on or after the operative date, but the engagement agreement may have been negotiated and executed some time prior to "commencement".
- Transitional relief for engagement agreements that were substantially drafted before the operative date but were executed after the operative date.

We would be pleased to discuss our comments with APESB and its staff. Should you wish to do so, please contact Chris George (christopher.george@au.ey.com or (02) 8295 6051).

Yours sincerely

Chris George
Oceania Assurance Professional Practice Director