KPMG

10 Shelley Street
Sydney NSW 2000

P O Box H67
Australia Square 1215
Australia

ABN: 51 194 660 183
Telephone: +61 2 9335 7000
Facsimile: +61 2 9335 7001
DX: 1056 Sydney
www.kpmg.com.au

Ms Merran Kelsall
The Chairman
Auditing and Assurance Standards Board
PO Box 204
Collins Street West
Melbourne VIC 8007

25 August 2014

Dear Ms Kelsall

Exposure Draft 01/14 Proposed Standard on Assurance Engagements ASAE 34XX *Assurance Engagements On Controls (Replacement of AUS 810)*

We are pleased to have the opportunity to comment on Exposure Draft 01/14 issued by the Australian Auditing and Assurance Standards Board.

We are supportive of the overall content of the Exposure Draft and the approach proposed by the AUASB.

We are very keen to provide our input into the development of this proposed standard.

The release of an assurance standard on controls in Australia is very important in the Australian landscape at this time and we support the AUASB in the release of the standard as soon as possible.

Our comments on the specific matters raised by the AUASB are set out below.

Comments in relation to specific matters raised by the Board

(1) Does this standard address the scope of all common engagements where assurance practitioners are requested, or required to provide assurance on controls?

Yes, the standard provides the flexibility required to address the numerous types of engagements that will be captured by this standard. We have three comments to add:

i. It is now standard practice to use service organisations so this should be considered more thoroughly throughout the standard and the examples. More detail on this comment is provided below.

ii. We believe there may be instances of assurance engagements on controls for a service organisation that cover controls relating to both financial reporting and operational or compliance controls. It would be helpful to consider how to apply the proposed standard and ASAE 3402 in this instance.

iii. We'd like to understand how this standard will interact with the regulatory requirements and relevant guidance statements such as GS 004, GS 012, etc. Will the guidance statements impacted by this standard be re-examined?

(2) Is it appropriate that all engagements are required to conclude on the suitability of the design to meet the identified control objectives and, in addition, may include:

(a) fair presentation of the description of the system (attestation engagements only);

(b) implementation of controls as designed; and/or

(c) operating effectiveness of controls as designed?

Yes, we believe it is appropriate to always include a conclusion on the suitability of design to meet identified control objectives with the option to include the other elements as listed above.

(3) Is it appropriate that the scope of a controls engagements may cover, either:

(a) a specified date for engagements including the description, design and/or implementation of controls; or

(b) throughout the specified period for engagements which include operating effectiveness of controls?

Yes, we agree that a specified date is suitable for engagements including the description, design and/or implementation of controls or throughout the specified period for engagements on operating effectiveness of controls.

We do note that there is no specified minimum period for assessing operating effectiveness of controls. This is different from a Service Organisation Controls ('SOC') report to provide information relative to a user entity's financial statement audit i.e. a Type 2 report ordinarily covers a minimum period of six months in order to be useful to user auditors.

Not having a specified minimum period allows for flexibility and judgement of the practitioner to potentially suit many engagement scenarios; however, we feel that it would be helpful to provide some considerations for the practitioner to consider what would be an appropriate period. These considerations may include:

- is the period suitable or meaningful to the intended users;
- whether the audit practitioner is engaged close to the date by which the report on controls is to be issued;
- the period for which the controls have been in operation i.e. a short period may result due to a new implementation;
- whether the responsible party has requested a specified period that may indicate bias i.e. scope exclusion that does not include instances of possible control deviations;
- whether certain control procedures leave evidence of their operation in the specified period; and
- if the practitioner has knowledge of deviations observed in prior engagements i.e. the practitioner may consider whether the period is broad enough to observe sufficient instances of the control in operation.

Also see ASAE 3402 paragraph A30.

(4) Are the considerations for conducting a direct engagement adequately differentiated from an attestation engagement?

Yes, it is well differentiated; however, there is a need for more information to help the practitioner make a well informed decision on how to structure these engagements. Describing these engagements from the perspective of the impact on the practitioner would be useful. For example, a direct reporting engagement is a higher risk engagement for the practitioner compared to an attestation engagement because it does not place as much focus and reliance on management's responsibilities or statement. It also has the potential to require a significantly larger work effort because the practitioner will likely develop the control objectives and determine which controls act together to address the control objectives. This could be substantially different from an attestation engagement where the control objectives and controls designed to meet them have been adequately described and evaluated.

Furthermore, the practitioner needs to carefully consider the intended users' needs in a direct reporting engagement and what control objectives are important to them. This may

be challenging where the practitioner does not have direct access to the intended users and it is not specified.

If this information is not able to be included in ASAE 34XX due to the issue of direct reporting not being addressed in the umbrella standard ASAE 3000 we ask that you consider providing separate guidance outside of this standard.

(5) Is the objective of an assurance practitioner in ASAE 3000 to obtain assurance about "whether the subject matter information is free from material misstatement" appropriately adapted for an engagement on controls to obtain assurance about whether there are material:

(a) misstatements in the description of the system;

(b) deficiencies in the suitability of the design to achieve the control objectives;

(c) deficiencies in the implementation of controls as designed; or

(d) deviations in the operating effectiveness of controls as designed?

Yes.

(6) Are the procedures required for limited and reasonable assurance appropriate and adequately distinguished?

Yes.

Paragraph 54.L on obtaining evidence regarding operating effectiveness of controls is particularly helpful as it indicates that limited assurance procedures may involve enquiring about and observation of the operation of the controls for a small number of transactions or events.

We do believe however that further considerations on whether limited or reasonable assurance is appropriate would be helpful for the practitioner. This should be linked to the intended user's needs and whether they have a sufficient understanding of the level of assurance that has been agreed. A14 touches on this but more guidance on the considerations in determining whether the level of assurance is meaningful would be helpful. The practitioner should ensure that the drivers for a limited assurance engagement are well understood.

Distinguishing between limited and reasonable assurance is still poorly understood in the market so practitioners need to be taking whatever reasonable steps they can take to reduce the expectation gap.

(7) Is a limited assurance engagement on controls a meaningful engagement?

Yes for limited assurance engagements to evaluate design, fair presentation of a system or implementation.

A practitioner needs to exercise caution around the appropriateness of accepting a limited assurance engagement evaluating operating effectiveness. The nature of the testing required may not be consistent with that typically performed for limited assurance engagements. The type of evidence a practitioner obtains to evaluate whether controls are operating effectively is similar whether the engagement is structured as limited or reasonable assurance.

(8) Are the appendices included appropriate and are sufficient example assurance reports included to address the most common engagements on controls?

We suggest it would be useful to provide an example long-form report.

Given the widespread and increasing use of service organisations in the market, all of the examples should provide example wording of either the inclusive or carve-out method. The engagement letter examples should cover the fact that if the inclusive method is used, the practitioner will require a representation letter from the service organisation.

It would also be useful to provide an example system description and attestation. This could be distinguished from the examples already provided in ASAE 3402 by focussing on a system description that does not relate to financial reporting, for example, cloud providers.

Similarly, it would be useful to provide an assurance report example that reflects paragraph 15 (a) (ii) and is a conclusion phrased in terms of the statement of the responsible party or evaluator. The examples in the appendix seem to be phrased in terms of 15 (a) (i) only.

Management Responsibilities

We suggest additional management responsibilities are included in both of the Engagement Letter examples to include informing the practitioner of any contentious issues/matters that will impact controls, violations or possible violations of laws or regulations that could have a material effect on the subject matter, any communications from regulators concerning non-compliance with or deficiencies in practices relating to the subject matter, and allegations of fraud or suspected fraud matters.

Other Matters

Example 2: **Engagement Letter for a Direct Engagement for Reasonable Assurance on the Design and Operating Effectiveness of Controls** seems to be missing the purpose of the engagement and the description of the intended users. This was very clear in the opening paragraph of Example 1.

The **Engagement Letter examples** don't include inherent limitations around projection of results into future periods although this is included in the assurance report examples. Given we talk about inherent limitations of an assurance engagement, it would be good to set expectations about the boundary of our conclusion.

The [Assurance Report] section of each of the **Engagement Letter examples** doesn't appear to cover all the requirements of paragraph 22 (a) (h).

Example 1 of Assurance Reports on Controls could be improved by having an example wording of the elements of a system description that are not covered by our conclusion. See paragraph 85 (d) (iii) for the requirement.

Assurance Practitioner's Responsibilities in **Example 1 Limited Assurance Report on Description and Design of the Entity's Controls as at a Specified Date**: Could the wording be phrased in more typical limited assurance wording? Alternate wording is provided below:

"That standard requires that we comply with relevant ethical requirements and plan and perform our procedures in order to state whether anything has come to our attention that would indicate in all material respects, that the description does not fairly present the system as designed and the controls stated in the description as at [date] were not suitably designed to achieve [[list overall objectives]/the control objectives identified] if the controls operated effectively."

Example 2: Reasonable Assurance Attestation Report on the Description, Design and Operating Effectiveness of the Entity's Controls throughout the Period: The opinion paragraph states:

(a) the description fairly presents the [*type or name of*] system as designed and implemented, throughout the period [*date*] to [*date*];

however; implementation is outside the scope of this example.

Example 3: Reasonable Assurance Report on the Design and Implementation of the Entity's Controls as at a Specified Date: suggest include an inherent limitation around future operating effectiveness.

Example 4: Reasonable Assurance Report on the Design and Operating Effectiveness of the Entity's Controls throughout the Period: The following statement should be in square brackets since this example is designed for both direct or attestation engagements.

ABC is responsible for

(b) identifying the control objectives;

Example Modified Assurance Reports on Controls Please see the suggested wording change for each example:

Our opinion/conclusion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion/conclusion were those identified in ABC's statement at page [*aa*]. [In our opinion/Based on the procedures we have performed and the evidence we have obtained], except for the matters described in the basis for qualified opinion/ conclusion above], in all material respects

(9) What, if any, are the additional significant costs to/benefits for assurance practitioners and the business community arising from compliance with the requirements of this proposed Standard? If there are significant costs, do these outweigh the benefits to the users of assurance services?

KPMG believes this standard will be welcomed by practitioners and those seeking our services.

(10) Are there any other significant public interest matters that constituents wish to raise?

Service Organisations and the Inclusive Method

The standard needs to further contemplate service organisations and the inclusive method in the *acceptance and continuance* paragraphs as well as *agreeing the terms of the engagement* and *representation letters* and *appendix examples* because of the unique considerations and the increased presence of service organisations in the market. If the engaging party is not the only responsible party, the practitioner needs to consider the effect of this on access to records, documentation and other information the practitioner may need to access to complete the assurance engagement.

This would include obtaining a representation letter from the service organisation for the matters within the scope of the audit. See paragraph A4 of ASAE 3402 which requires the practitioner to obtain – when using the inclusive method - agreement regarding the matters in paragraph ASAE 3402 13 (b) (i)-(iv) as applied to the subservice organisation.

This paragraph is also important to practitioners because it highlights that the inclusive method is generally feasible only if the service organisation and the subservice organisation are related, or if the contract between the service organisation and the subservice organisation provides for its use. This is an important consideration upon accepting an inclusive method engagement under ASXX and how the practitioner agrees to structure it.

Use of Internal Audit Function

Please include more guidance or wording on whether direct assistance is expressly prohibited. More clarity on this issue will help practitioners determine how to work with internal audit and the appropriate boundary of our reliance on them.

Observations and Typos

1 Terminology between "opinion" and "conclusion" needs to be referred to consistently throughout the standard and the appendices. See 4 (d), 4 (g);

2 Paragraph 4 (g) (ii) needs same style with bullets a, b, c applied to it similar to (i) above;

3 Paragraph 4 (g) (ii) should say "throughout a specified period" rather than throughout the….;

4 Paragraph 6 (a) should this be "overall" control objectives? These engagements don't just address overall objectives;

5 Paragraph 6 (b) "compliance with regulatory requirements ~~**for controls assurance**~~, such as";

6 Paragraph 6 (b) (ii) small L required on legislative;

7 Paragraph 6 (c) should say ", except for **controls related to financial reporting**"…..;

8 Paragraph 6 (d) voluntary engagements initiated by the entity on its own controls over services, activities undertaken or functions which it provides;

9 Paragraph 8: Please explain as 3000 does not address direct engagements;

10 Paragraph 13 (b) should say "…which expresses either **a** reasonable or limited assurance **conclusion** and describes the basis for the conclusion;

11 Paragraph 14 (a) could be written more clearly. "for an attestation engagement, is conducted by the responsible party or evaluator, and presented as **an evaluation of the design and/or** the description……;

12 Paragraph 14 (b) "as there is no statement ~~**provided to the assurance practitioner**~~ **prepared by the responsible party** in a direct engagement";

13 Paragraph 15 (a) "The outcome of that evaluation is provided in a **statement to the assurance practitioner**, which either is available to the intended users of the assurance report or may be presented by the assurance practitioner in the assurance report." Shouldn't the outcome be provided to the intended user, not the practitioner?

14 Paragraph 15 (a) (i) and (ii). Is the phrase "and the control objectives" needed in either bullet here?

15 Paragraph 15 (g) Refer readers to Appendix 1;

16 Paragraph 15 (k) Should read "deviation in operation **effectiveness** of controls";

17 Paragraph 15 (u) Should read …"which is subject to the **assurance** engagement";

18 Paragraph 15 (gg) should read "conveys the assurance practitioner's **conclusion**". Currently says "opinion";

19 Paragraph 20: (b) should include the assertions completeness and accuracy of the description

20 Paragraph 21 (b) "issue a modified conclusion…" Please indicate what form of modified conclusion. Refer to ASA 705;

21 Paragraph 22 (a) (i). for identifying control objectives and **the risks that threaten achievement of those control objectives**; The yellow highlighted phrase should be a separate point;

22 Paragraph 25: See suggested changes: "If law or regulation prescribe the criteria for evaluation of the relevant controls or the ~~layout or wording of the~~ **form and content of the** assurance report, the assurance practitioner evaluates the criteria and **form and content of the assurance** report ~~wording~~. If the criteria are unsuitable or if **in the opinion of the assurance practitioner**, intended users might misunderstand the assurance ~~conclusion~~ report, the assurance practitioner shall:"

23 Paragraph 33: This paragraph needs to address the concept of "clearly trivial to accumulated misstatements". See ASA 450 paragraph A2;

24 Paragraph 34 (d) (ii): The phrase "the controls were not implemented as designed" should be a separate point;

25 Paragraph 36: Delete: "~~During the planning phase~~" and replace with "In planning the engagement";

26 Paragraph 37: Replace "an effective internal audit function ~~will often enable~~" and replace with "may";

27 Paragraph 40 (g) Is this relevant only if it's in scope?

28 Paragraph 43 and 44: is this worded appropriately to assurance on controls?

29 Paragraph 45 (c) Presume this means "when controls change in period". This could be worded better;

30 Paragraph 46R (c) How different is this to 35 which would apply to limited assurance as well?

31 Paragraph 48: "If the scope of the engagement includes assurance on the entity's description of the system'. What if the engagement is direct assurance?

32 Paragraph 48 (f) "in the case of a report covering operating effectiveness of controls". Why in this circumstance only?

33 Paragraph 51R (h): determining a means of selecting items for testing that is ~~effective~~ **appropriate**";

34 Paragraph 57:"…..and consider whether the new controls have been in place for a sufficient period to assess their effectiveness". Why only perform this assessment for new controls?

35 Paragraph 59: (b) "misstatements **or omissions** in the description of the system";

36 Paragraph 59: "deficiencies in the implementation as designed" should be a separate point i.e. new bullet;

37 Paragraph 60: "maybe" should be written "may be"; Paragraph doesn't address "other than those that are clearly trivial";

38 Header above paragraph 61 should be "Misstatements **or Omissions** in the Description of the System"

39 Paragraph 62 should address concept of 'clearly trivial";

40 Paragraph 64 (b) "additional testing of the control or of other **compensating/indirect** controls is necessary….";

41 Paragraph 64 (c) "The testing that has been performed….." should distinguish between limited and reasonable assurance;

42 Paragraph 68 "If the assurance practitioner identified a control deficiency or deviation, whether in the design, implementation or operating effectiveness of that control". This should include the "Description" as well;

43 Paragraph 69 "if the assurance practitioner ……" should include "description" as well;

44 Paragraph 71 and 72: should these paragraphs be considered earlier;

45 Paragraph 76 (d) (ii): "misstatements **or omissions** in the description of the system";

46 Paragraph 80: "……shall disclaim their conclusion if the possible effects….." This needs to include **adverse** conclusion as well;

47 Paragraph 81 (b) "misstatements **or omissions** in the description of the system";

48 Paragraph 82 "the assurance practitioner shall identify any compensating/**indirect** controls";

49 Paragraph 83 "or operating effectiveness of controls, which are material ~~alone~~ **individually** or in combination, on the assurance practitioner's conclusion";

50 Paragraph 85 (h) is missing (i) reference;

51 Paragraph 85 (k) (iv) "when the assurance practitioner expresses a modified conclusion, the assurance report shall contain….. " needs to discuss requirement for inclusion of "Basis for Modified Opinion";

52 Paragraph 86: Need to follow ASAE 3000 principles for long form reporting;

53 Paragraph 94 needs to include file assembly;

54 Paragraph A19: “for evaluating implementation **and operating effectiveness** of controls”;

55 Paragraph A32: Comparative work effort: least detailed ~~testing~~ **evidence**, moderate detailed ~~testing~~ **evidence**, most detailed ~~testing~~ **evidence**;

56 Paragraph A33: maybe should be “may be”;

57 Paragraph A42: “not affected by the level of assurance being ~~provided~~ **obtained**”;

58 Paragraph A63 2nd bullet and 3rd indented bullet: should “date” be “data”;

59 Appendix 1: Criteria for evaluating subject matter: the criteria for fair presentation of description of the system should include concepts of completeness and accuracy of the description;

60 Appendix 4: example 1: “our assurance engagement will be conducted with the objective of our expressing an **opinion**”. Prefer not to say “express an opinion”;

61 Appendix 4: example 1: “the work undertaken by us to form an **opinion** ~~**is permeated**~~ **requires** ~~**by**~~ judgment”. Prefer not to say “form an opinion”;

62 Appendix 4: example 1: “Assurance procedures” paragraph (e) performing tests of controls to ascertain whether the degree of compliance…….” This is referring to operating effectiveness. Consider changing the terminology;

63 Appendix 4: example 1: Material misstatements in description, deficiencies in design or deviations in operating effectiveness of controls: we will issue an assurance report without modification……..where our procedures do not ~~disclose~~ **identify** a material misstatement”;

64 Appendix 4: example 1: Under header of “Distribution of the Assurance Report” is actually missing the sentence on “should not be distributed to parties other than …..”;

65 Appendix 4: example 1: Material misstatements in description, deficiencies in design or deviations in operating effectiveness of controls: Although the primary purpose of our assurance engagement …….we ~~will~~ **may** also periodically provide you”;

66 Appendix 6: Example 1: ABC is responsible for (b) “**method of presentation**”. Please clarify, what does this mean? Do you mean basis of preparation?

67 Appendix 6: Example 1:”The procedures performed in a limited assurance engagement…… and are **different in nature** and less in extent than for, a reasonable”;

68 Appendix 6: Example 1: Paragraph on page 87 “Also, a limited assurance engagement does not provide all evidence…….” is a repeat of the paragraph above. Remove duplication;

69 Appendix 6: Example 1: Missing the Distribution paragraph on page 87. Has Intended Users and Purpose but missing distribution;

70 Appendix 6: Example 2: Page 89 refers to “method of presentation of the description”. Terminology check here;

71 Appendix 6: Example 2: Page 89 is missing the distribution paragraph;

72 Appendix 6: Example 3: Page 92 is missing the distribution paragraph;

73 Appendix 6: Example 4: Page 94 is missing the distribution paragraph;

74 Appendix 7: Suggest this is just included for reasonable assurance. The wording for the "Qualified Opinion/Conclusion does not work well for limited assurance;

75 Appendix 7: Example 1: the wording in (b) "except for the matter described in the Basis for Qualified Opinion…." is not prominent enough;

76 Appendix 7: Example 2: The Qualified Opinion/Conclusion does not work well for limited assurance;

77 Appendix 7: Example 2: (a) "except for the matter described in the Basis for Qualified Opinion/Conclusion" should be up front;

78 Appendix 7: Example 3: Qualified Opinion should be Qualified Opinion/Conclusion similar to the header above;

79 Appendix 7: Example 4: Typo. "Consequently, we were unable to determine whether the stated control ~~objective~~ operated effectively…";

80 Appendix 7: Example 4: (c) "except for the matter described in the Basis for Qualified….." should be more prominent.

Further Questions:

Paragraph A18: control objectives can be developed for sale on a proprietary basis? What is an example of this?

Paragraph A25 looks to be the same paragraph as A19?

Paragraph A88 is a key paragraph but is buried in the standard. This should be more prominent. It states that if the engagement covers operating effectiveness, then implementation is not usually separately tested or concluded upon unless specifically included in the terms of engagement. This is a premise that is then followed through all the subsequent examples.

Please contact Jennifer Travers on (03) 9288 5015 if you wish to discuss these comments further.

Yours sincerely

Martin McGrath

Partner