November 25, 2020

Mr. Tracy Harding
Auditing Standards Board
American Institute of Certified Public Accountants
1211 Avenue of the Americas
New York, NY 10036-8775

RE: Proposed Statement on Auditing Standards *Understanding the Entity and its Environment and Assessing the Risks of Material Misstatement*

Dear Mr. Harding:

We appreciate the opportunity to provide comments on the Auditing Standards Board’s (the Board) Proposed Statement on Auditing Standards *Understanding the Entity and its Environment and Assessing Risks of Material Misstatement* (Proposed SAS). We support the overall objective of the Proposed SAS and we believe the concept of a risk-based audit is critical to fostering audit quality. Proper identification of the risks specific to an engagement provide an auditor with the ability to scope the audit and respond to risks to reflect facts and circumstances and to focus the audit efforts commensurate with the assessed risk. We understand that the requirements and guidance within this Proposed SAS reflect the Board’s objective to converge with the equivalent international auditing standards, and believe that additional guidance to clarify the auditing requirements and application guidance would be helpful in the U.S.

Our overall feedback on the Proposed SAS is set out below. The appendix to this letter includes feedback to selected issues for which the Board has requested comment.

**Auditors’ ability to consistently apply the principles in the Proposed SAS**

We believe that risk assessment is an important avenue for scaling an audit to the risks applicable to a particular engagement. For example, if an entity is less complex, proper risk assessment allows the auditor to design the audit procedures to reflect the lower risk and focus procedures on those risks applicable to the entity and its circumstances. The Proposed SAS addresses scalability by incorporating application guidance and examples for less complex entities. However, the requirements themselves are, in some cases, overly general and may lead to inconsistent application. Given that risk assessment is fundamental to the success of a risk-based audit, we believe additional guidance is needed to define or clarify critical concepts. For example, the Proposed SAS does not indicate the procedures an auditor needs to perform to “obtain an understanding” which is fundamental to effective risk assessment. It is important for auditors to have clear and executable guidance that can be the basis for a compliant methodology for risk assessment that allows them to develop the appropriate audit responses to the risks identified and design and perform procedures to support a conclusion at a level of reasonable assurance.
Obtaining an understanding of the entity and its environment, the applicable financial reporting framework, and the entity’s system of internal control

We agree that obtaining an understanding of an entity and its environment, the applicable financial reporting framework, and the entity’s system of internal control are key aspects of properly designing and performing a risk-based audit. We believe the alignment of the components of a system of internal control with COSO (2013) or another established framework is beneficial as it provides familiar concepts related to an auditor’s evaluation of the system of internal control and assessment of risks of material misstatement. Outlining the various components within the standard without reference to a framework (whether COSO (2013) or another framework) makes it difficult for the auditor to evaluate the components of internal control. In order to drive a consistent and thorough understanding of an entity’s system of internal control, the auditor should use a suitable, recognized framework.

Additionally, further guidance is needed to 1) include requirements to identify controls within the various components, 2) address how controls identified within each component should be evaluated, and 3) articulate the impact this evaluation has on the nature, timing, and extent of audit procedures.

The information system

Obtaining an understanding of and evaluating IT is a part of a robust risk assessment process. However, we note that the Proposed SAS is inconsistent in its descriptions of risks arising from IT, GITCs, IT applications, and information processing. We believe the standard should focus on the automated control activities implemented within IT applications and how GITCs support the consistent functioning of those controls. This will better align the risk assessment procedures performed over information systems with the relevant audit response. Additionally, the appendices focused on IT include unspecified assumptions that may mislead auditors trying to identify the relevant aspects of IT systems and controls in scenarios of varying complexity.

* * * * * * * * * * * *

We appreciate the Board’s consideration of our comments in support of enhancing auditing standards and audit quality. If you have any questions regarding our comments included in this letter, please do not hesitate to contact Harry Cohen at 212-954-3293 or hcohen@kpmg.com or Matt Doyle at 212-954-2187 or mrdoyle@kpmg.com.

Sincerely,

KPMG LLP
Appendix – Responses to specific questions

1 Are the requirements and application material of the proposed SAS sufficiently scalable, that is, is the proposed SAS capable of being applied to the audits of entities with a wide range of sizes, complexities, and circumstances?

— Paragraph 9 of the Proposed SAS notes that AU-C 200 addresses the fact that some AU-C sections include scalability considerations. We agree that scalability is an important attribute of a risk assessment standard, as any audit should be tailored to address the risks specific to the entity being audited regardless of the complexity of that entity. However, we propose to edit paragraph 9 as follows to clarify that scalability considerations illustrate how the guidance might be scaled to address various levels of complexity.

9. AU-C section 200 states that some AU-C sections include scalability considerations, which illustrate the how application of the requirements of a standard might be applied to all entities regardless of whether their nature and circumstances are less or of varying levels of complexity or more complex. This proposed SAS is intended for audits of all entities, regardless of size or complexity; therefore, the application material incorporates considerations specific to assessing risks for both less complex entities and as well as more complex entities, where appropriate. Although the size of an entity may be an indicator of its complexity, some smaller entities may be complex, and some larger entities may be less complex.

— Throughout the proposed guidance, the term used is often “size and complexity” which could continue to lend more weight to an entity’s size. Consider removing size as an indicator throughout the standard (for example, as amended above in paragraph 9) to reiterate that size does not equate to complexity.

— We support the application guidance related to scalability, especially removal of “Considerations Specific to Smaller Entities” headers, as small entities can be complex and large entities can be simple. We also support the inclusion of appendices that outline various scalability considerations, and specific illustrations and examples of considerations for entities of varying complexity. As noted in our response to question 3 below, we believe changes are needed to some of the appendices to provide appropriate guidance related to applying the audit requirements.

— In paragraph A21, the application guidance notes that when systems and processes lack formality, “the auditor may still be able to perform risk assessment procedures through observation and inquiry.” As written, the application guidance does not address considerations when the auditor is unable to perform suitable risk assessment procedures or when the necessary control structure does not exist. Furthermore, the guidance is inconsistent in the use of “observation and inspection” versus “observation or inspection.” We acknowledge there are entities with less formal internal control over financial reporting. In those instances, the extent of documentation to inspect may be limited, and we believe that performing only inquiry and observation as elements of a practitioner’s risk assessment may not provide sufficient information to identify and evaluate risks. The Proposed SAS should include guidance on the nature of the procedures to be performed in these situations.
We suggest introducing, in paragraphs A58-A61, the concept that if you have two entities of similar nature and complexity, but one has a more robust control structure (including its control environment, risk assessment, monitoring and information and communication processes), the risks associated with it may be lower than one lacking that structure. This could impact the auditor’s determination of whether it is appropriate to take a controls reliance approach and the nature, timing, and extent of procedures needed to obtain sufficient, appropriate audit evidence.

2 Do the proposals made relating to the auditor’s understanding of the entity’s system of control assist with understanding the nature and extent of the work effort required and the relationship of the work effort to the identification and assessment of the risks of material misstatement? Specifically:

a. Have the requirements related to the auditor’s understanding of each component of the entity’s system of internal control been appropriately enhanced and clarified? Is it clear why the understanding is obtained and how this informs the risk identification and assessment process?

— Obtaining an understanding of each of the components of internal control is important and we acknowledge that the explanations in each section as to why it is important to gain an understanding of the components are helpful. However, as noted above, the requirements do not provide the auditor guidance to determine what procedures should be performed to obtain a sufficient “understanding” of the various components. The standard states in paragraph A100 that inquiry alone is not sufficient to obtain an understanding of the control environment, entity’s risk assessment process and entity’s process to monitor the system of internal control. However, it is not clear what procedures might be appropriate. Extant AU-C 315.14 explicitly states that when obtaining an understanding of internal controls that are relevant to the audit, the auditor should evaluate the design of those controls and determine whether they have been implemented. We recommend retaining that concept in the revised standard, noting that “relevant controls” includes controls within all components of internal control over financial reporting or otherwise adding examples of what procedures may be acceptable to gain an understanding of the entity’s system of internal control.

— The requirements for obtaining an understanding of the relevant processes for risk assessment, monitoring, and information and communication do not include obtaining an understanding of controls within those processes. It is important to delineate between “processes” and “controls” as this is an area of common confusion in practice and both are integral to the auditor’s understanding of the system of internal control. Paragraphs 22, 24, and 25 should include language similar to that in paragraph 21 that the auditor should obtain an understanding of “the set of controls, processes, and structures” relevant to each component. See additional comments in our response to question 3 below related to observations on the need to delineate IT applications from the related controls.

b. Have the requirements related to the auditor’s identification of controls that address the risks of material misstatement been appropriately enhanced and clarified? Is it clear how controls that addressed the risks of material misstatement are identified, particularly for audits of smaller and less complex entities?

See comments above related to requirements for identifying and evaluating controls and shifting the focus on scalability away from “smaller” entities.
c. Given that COSO's 2013 Internal Control—Integrated Framework (COSO framework) is often used by entities subject to the AICPA’s generally accepted auditing standards, is the terminology in paragraphs 21–27 and related application material of the proposed SAS clear and capable of consistent interpretation for audits of entities that use the COSO framework?

The terminology used in paragraphs 21-27 is consistent with the components identified in the COSO framework. However, in order to obtain an appropriate understanding of each component, we recommend including language in paragraph A102 allowing the auditor to identify and use a suitable framework to evaluate the control components as follows: “Management might use an internal control framework with components that differ from the components identified in this Standard, or those specified by COSO when establishing and maintaining the entity's system of internal control. In some instances, management may not use a framework at all. In obtaining an understanding and evaluating the entity’s system of internal control, the auditor may use the framework used by management or another suitable, recognized framework such as COSO.”

3 Are the enhanced requirements and application material related to the auditor’s understanding of the IT environment, the identification of the risks arising from the entity’s use of IT, and the identification of general IT controls clear to support the auditor’s consideration of the effects of the entity’s use of IT on the identification and assessment of the risks of material misstatement?

— We support including enhanced application material and agree it is beneficial for the concept of evaluating IT risks. In order to help achieve that objective, we suggest certain changes or additions outlined.

— The term “information processing controls” is used throughout the proposed SAS. The definition of information processing controls has been changed significantly from that in extant AU-C 315, and appears to introduce a new control category that includes a subset of manual and automated controls. It is unclear within the proposed standard what is the link between GITCs and information processing controls given that information processing controls can be manual, and how this impacts risks associated with IT. We suggest focusing on application controls and GITC and including additional guidance in the control activity section regarding the need to identify and evaluate controls over the input, integrity, and extraction of information from the information systems. Further, paragraphs A184 and A251 address testing operating effectiveness of GITCs and the impact that may have on control risk and planned audit response. However, these paragraphs do not clearly state that an auditor should not rely on application controls without effective GITCs. We suggest the following edits:

A184 . . . if information-processing controls depend on general IT controls, the auditor may determine to test the operating effectiveness of the general IT controls, which will then require the design of tests of controls for such general IT controls. If, in the same circumstances, the auditor determines not to test the operating effectiveness of the general IT controls, or the general IT controls are expected to be ineffective, the auditor does not rely on the automated controls dependent on such general IT controls, and the related risks arising from the use of IT of material misstatement may need to be addressed through the design of substantive procedures.”

A251. When the auditor plans to test the operating effectiveness of an automated control, the auditor may also plan to test the operating effectiveness of the relevant general IT controls that support the continued functioning of that automated control to address the risks arising from the use of IT, and to provide a basis for the auditor’s expectation that the
automated control operated effectively throughout the period. When the auditor expects
related general IT controls to be ineffective, this determination may affect the auditor’s
assessment of control risk at the assertion level, and the auditor’s further audit procedures
may need to include substantive procedures to address the applicable risks arising from the
use of IT to material misstatement. Further guidance about the procedures that the auditor
may perform in these circumstances is provided in AU-C section 330.

— Paragraph A187 and paragraph 10 of Appendix E allow the auditor an option to directly test the
inputs and outputs of the report generation process, or to test management’s controls over the
completeness and accuracy of the report. It is not clear whether direct testing could be applied
both in cases when the auditor is not relying on controls and when the auditor is relying on
controls. We believe that direct testing is only appropriate when the auditor is not relying on
controls that depend on the report, to prevent inappropriate reduction of substantive testing from
inadvertent control reliance when management’s controls over reports have not been tested. For
example, management may use a system-generated report in the operation of a specific control,
such as the review of an accounts receivable aging to determine the valuation of accounts
receivable. Management has a responsibility to design and operate controls over the accuracy and
completeness of the data and information used and provided by the system generated report. If
the auditor direct tests the report while placing reliance on the management review control, the
auditor could conclude that the review control is operating effectively without having tested
whether management has validated the relevance and reliability of the data and information used
in the control. Said another way, direct testing reports while taking a control reliance approach is
an example of performing a substantive procedure to address risks arising from the use of IT,
which is not appropriate. Accordingly, we suggest the following edits to paragraph A187:

The controls identified by the auditor may depend on system-generated reports, in which
case, the IT applications that produce those reports may be subject to risks arising from the
use of IT. If the auditor is relying on the controls using such reports, the controls over the
completeness and accuracy of those reports are subject to the requirements in paragraphs
26c-d. In other cases, when the auditor may plan not to does not rely on controls, over the
system-generated reports and plan to the auditor may instead directly test the inputs and
outputs of the report generation process for reports used as part of substantive procedures.
In this case, the auditor may identify the related IT applications as not being subject
to risks arising from IT and, thus, these controls may not be subject to the requirements in
paragraphs 26c–d.

— The table in Appendix E describes examples of typical characteristics of specific types of IT
applications. While paragraph 4 of this Appendix states that the characteristics are “directional
and may differ depending on the nature of the specific IT applications in use” we believe that the
use of “N/A” (not applicable) for certain matters is not directional and may be construed as a
conclusive determination. For example, the first row in the table in Appendix E implies that for a
purchased application with no customization, it is not necessary to evaluate the extent of
automated procedures for processing. Regardless of whether an application is purchased or
highly customized, it will include some level of automated procedures for processing. Therefore,
labelling this category as “N/A” is misleading. We recommend that the characteristics be
described directionally for all matters (such as lower, moderate, higher), with increasing
complexity as the table moves from “purchased applications with no customization” through
“custom-developed applications or more complex ERP applications with significant
customization.”
The table in Appendix F illustrates whether specified risks and controls are expected to be applicable to specific types of IT applications. We again believe that the determinations of applicability are presented as conclusive when they are, in fact, dependent on facts and circumstances that have not been presented. For example, consider row A. from the below excerpt:

<table>
<thead>
<tr>
<th></th>
<th>Purchased applications with no customization</th>
<th>Purchased applications or simple legacy or low-end ERP applications with little or no customization</th>
<th>Custom developed applications or more complex ERP applications with significant customization</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.</td>
<td>Segregation of duties is monitored, and conflicting access is either removed or mapped to mitigating controls, which are documented and tested.</td>
<td>N/A – no system enabled segregation</td>
<td>Yes</td>
</tr>
<tr>
<td>B.</td>
<td>Privileged-level access (for example, configuration, data and security administrators) is authorized and appropriately restricted.</td>
<td>Yes – likely at IT application layer only</td>
<td>Yes at all layers of IT environment for platform</td>
</tr>
</tbody>
</table>

Our experience has shown that the majority of systems have the ability to enforce segregation of duties, regardless of the level of customization or complexity and thus we believe this applicability guidance is inaccurate. While this is just one example, the same concept applies throughout the entire table. There is a risk that an auditor may inappropriately rely on the applicability as shown in this table based solely on the specific type of IT application and not appropriately identify the IT risks. This could result in the auditor not designing an appropriate audit response to those risks. Additionally, similar to the earlier discussion, this table focuses on the IT application as a whole, rather than considering the risks arising at the level of the automated controls identified to be responsive to a risk of material misstatement. For example, row B. from the above table indicates consideration only at the application layer in the “purchase application with no customization scenario”. To the extent a database is used in the execution of the control, segregation of duties should also be considered at the database layer. Lastly, we do not believe it is appropriate to assume that controls such as vulnerability scans of the network perimeter and investigation of threat alerts by intrusion detection systems at the network layer are a default or expected General IT Control, even for more complex IT systems. This risk should be considered for each layer based on the specific facts and circumstances, and it should not be implied that it is required. This would be an increase in the scope of most audits. We suggest that this table be revised to contemplate the differences in facts and circumstances even among like IT applications, or that a detailed fact pattern assumed for each IT application is presented.
5 Do you support the introduction of the spectrum of inherent risk into the proposed SAS?

We believe that the introduction of the spectrum of inherent risk is a more comprehensive picture of risk of material misstatement. However, the Proposed SAS only mentions that inherent risk can be higher or lower. This may cause confusion and suggest to auditors that inherent risk only consists of these two categories. While we do not think risk levels should be explicitly described within the standard, it would be beneficial to add the concept to paragraphs A230 – A236 that a risk associated with an assertion could fall anywhere from no/remote risk to significant risk and that categories other than “higher” and “lower” may be identified. Further it should be specified in this section of the application guidance that auditors can apply judgment to determine the categories to be used to reflect a risk’s relativity on the spectrum (e.g. low, medium, elevated, high, significant, etc.).

6 Do you support the separate assessments of inherent and control risk in relation to all risks of material misstatement at the assertion level?

We agree with the requirement to separately assess inherent risk and control risk included in the Proposed SAS, as these are two integral pieces of the audit risk formula. We believe that it is important for auditors to understand the concept that inherent risk is assessed regardless of the existence or effectiveness of controls. Likewise, we believe auditors should understand how their plans to rely on controls affect the nature, timing, and extent of procedures.

The proposed requirements do not link the objective of obtaining an understanding of the components of internal control to how it affects risk assessment. While inherent risk should not be dependent on the existence or operating effectiveness of control activities, the auditor’s understanding of the system of internal control can influence the nature, timing and extent of planned procedures. When there are deficiencies identified in other components of internal control, it may highlight an increased chance of material misstatements occurring. We suggest adding this concept to the relevant application guidance starting at paragraph A227.

7 What are your views regarding the clarity of the requirement to assess the control risk, in particular, when the auditor does not plan to test the operating effectiveness of controls?

While paragraph 34 outlines the effect of not testing operating effectiveness of controls on the auditor’s control risk assessment, it is not clear that if we plan to test operating effectiveness, our control risk assessment is based on our understanding of the design and implementation of the controls and an expectation that the controls are operating effectively. Paragraph A248 discusses this concept; however, we believe it should be explicitly stated in the requirements. We acknowledge that the requirement to reassess risk conclusions is in paragraph 37, but as the process is iterative instead of linear, the impact of controls that are not operating effectively should be introduced in the control risk section. Additionally, the wording in paragraph A248 that the auditor confirms the original control risk assessment implies that the result will support the initial conclusion. We suggest editing paragraphs 34 and A248 as follows:

34. The auditor should take into account the evidence obtained from understanding internal control when assessing control risk. If the auditor plans to test the operating effectiveness of controls, the auditor should assess control risk. If the auditor does not plan to test the operating effectiveness of controls, or the auditor concludes the controls are not operating effectively, the auditor’s assessment of control risk should be such that the assessment of assesses the risk of material misstatement is to be the same as the assessment of inherent risk.
A248. The auditor’s plans to test the operating effectiveness of controls is based on the expectation that controls are operating effectively, and this will form the basis of the auditor’s assessment of control risk. The initial expectation of the operating effectiveness of controls is based on the auditor’s evaluation of the design and the determination of implementation of the identified controls in the control activities component. Once the auditor has tested Depending on the results of tests of operating effectiveness of the controls in accordance with AU-C section 330, the auditor will be able to confirm the determination whether the initial expectation about the operating effectiveness of controls remains appropriate. If the controls are not operating effectively as expected, then the auditor will need to revise the control risk assessment in accordance with paragraphs 34 and 37.

8 What are your views regarding the clarity of the requirement in paragraph 26d of the proposed SAS to evaluate design and determine implementation of certain control activities (including, specifically, the requirement related to controls over journal entries)?

We support the requirements in 26d, including the requirement to evaluate the design and implementation of controls over journal entries. We suggest clarifying paragraph A176 to reflect the application of the requirement as follows:

A176. Controls over journal entries that address risks of material misstatement at the assertion level that are expected to be identified, and the design and implementation evaluated, for all audits are controls over journal entries because the manner in which an entity incorporates information from transaction processing into the general ledger ordinarily involves the use of journal entries, whether standard or nonstandard, or automated or manual. Paragraph 25a requires the auditor to obtain an understanding of the flows of information in the entity’s information system for significant classes of transactions, account balances, and disclosures. The understanding required by paragraph 26a(ii) includes controls over adjustments to significant classes of transactions, account balances, and disclosures in addition that may not be subject to controls over processing of routine transactions. In an audit where Further, the auditor may have has not identified no any related party or other transactions that meet the definition of significant unusual transactions in accordance with AU-C section 240, other significant risks, or other risks of material misstatement for which it is necessary for the auditor to evaluate the design of controls and determine that they have been implemented. In such an audit, the auditor may determine that there are no identified relevant controls other than the entity’s controls over journal entries.

9 Do you support the revised definition, and related material, on the determination of significant risks? What are your views on the matters previously presented relating to how significant risks are determined based on the spectrum of inherent risk?

We generally support the revised definition and related material. We suggest the following edits to Paragraph A240 to reflect that reporting key audit matters is only applicable if we are so engaged, and that timely review by the engagement partner is not dependent on the risk spectrum:

A240. Timely review of audit documentation by the engagement partner at the appropriate stages during the audit allows significant matters, including significant risks, to be resolved on a timely basis to the engagement partner’s satisfaction on or before the date of the auditor’s report. Additionally, the determination of significant risks allows for the auditor to focus more attention on those risks that are on the upper end of the spectrum, through the performance of certain required responses, including the following:
— Controls that address significant risks are required to be identified in accordance with paragraph 26a(i) of this proposed SAS, with a requirement to evaluate whether the control has been designed effectively and implemented in accordance with paragraph 26d of this proposed SAS.

— AU-C section 330 requires controls that address significant risks to be tested in the current period (when the auditor intends to rely on the operating effectiveness of such controls) and substantive procedures to be planned and performed that are specifically responsive to the identified significant risk.

— AU-C section 330 requires the auditor to obtain more persuasive audit evidence the higher the auditor’s assessment of risk.

— AU-C section 260 requires communicating with those charged with governance about the significant risks identified by the auditor.

— AU-C section 701, Communicating Key Audit Matters in the Independent Auditor’s Report, if applicable, requires the auditor to take into account significant risks when determining those matters that required significant auditor attention, which are matters that may be key audit matters.

— Timely review of audit documentation by the engagement partner at the appropriate stages during the audit allows significant matters, including significant risks, to be resolved on a timely basis to the engagement partner’s satisfaction on or before the date of the auditor’s report.

— AU-C section 600 requires more involvement by the group engagement partner if the significant risk relates to a component in a group audit and for the group engagement team to direct the work required at the component by the component auditor.

10 What are your views about the proposed stand-back requirement in paragraph 36 of the proposed SAS and the conforming amendments proposed to paragraph .18 of AU-C section 330?

We are supportive of the stand-back requirement and conforming changes to AU-C 330. Risk assessment is an iterative process and requiring auditors to take a step back and revisit previous conclusions on risks of material misstatement will help drive the appropriate identification of relevant assertions for significant classes of transactions, account balances, and disclosures. In cases where the auditor has identified material classes of transactions, accounts or disclosures that do not have an associated risk of material misstatement, it is appropriate to include a specific requirement for the auditor to evaluate whether that conclusion remains appropriate. Additionally, we support the changes made to paragraph 18 of AU-C 330, as those changes reflect alignment with the risk-based approach.

11 What are your views with respect to the clarity and appropriateness of the documentation requirements?

We are generally supportive of the documentation requirements. However, we note that paragraph 38b requires documentation of compliance with the guidance in paragraphs 19, 21, 22, 24, and 26. Paragraph 19b requires obtaining an understanding of the financial reporting framework, while paragraph 20 requires evaluating whether that framework is appropriate. For the components of ICFR, the evaluation requirement is a sub-bullet included with obtaining the understanding and is therefore included in the documentation requirements listed. We believe that the documentation requirements should include the auditor’s understanding of the framework as well as their evaluation as to whether the framework is appropriate. We suggest including paragraph 20 in the documentation requirement.
Further, we note that paragraph 23 addresses circumstances when the auditor identifies risks of material misstatement that management failed to identify, including requirements to determine whether any such risks are of a kind that the auditor expects would have been identified by the entity’s risk assessment process and, if so, obtaining an understanding of why the entity’s risk assessment process failed to identify such risks of material misstatement. We believe these items should also be documented by the auditor and thus, paragraph 23 should be included in the documentation requirements of paragraph 38b.

We also note that paragraph 25 requires obtaining an understanding of the information system and communication and, in particular, paragraph 25c requires an evaluation of the information gleaned from obtaining this understanding to determine if the information system is appropriate. As paragraph 38e specifically addresses control activities in paragraph 26, we believe the reference in paragraph 38b should be to paragraph 25 instead, which would be consistent with ISA 315.